NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WINDOW OF OPPORTUNITY: MITIGATING THREATS FROM DISRUPTIVE TECHNOLOGIES BEFORE WIDESPREAD ADOPTION

by

Christopher R. Knapp

September 2014

Thesis Advisor: Rodrigo Nieto-Gómez
Second Reader: Carolyn Halladay

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
WINDOW OF OPPORTUNITY: MITIGATING THREATS FROM DISRUPTIVE TECHNOLOGIES BEFORE WIDESPREAD ADOPTION

5. FUNDING NUMBERS

6. AUTHOR(S) Christopher R. Knapp

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

As the pace of technology increases, so does the potential development of disruptive technology-related threats. However, by enacting proactive safety and security measures during the window of opportunity, a government can cost-effectively protect an unsuspecting and ill-prepared society before an emerging disruptive technology is widely adopted without stifling its future development.

The basis for the threat mitigation approach described herein is to inject the protective measures into the innovation cycle prior to a technology being adopted by the early majority in Everett Rogers's technology adoption cycle. This period of time (the window of opportunity) occurs when the GartnerGroup's hype cycle's trough of disillusionment aligns with Geoffrey Moore's chasm.

This thesis explores two possible courses of action for mitigating domestic security and safety threats once a new technology's window of opportunity is identified. First, domestic law enforcement can use this information to mitigate future security and safety concerns. Second, the state could design a flexible regulatory framework around the window in order to provide innovators and producers of an emerging disruptive technology with information highlighting its potential for illicit appropriation.

14. SUBJECT TERMS innovation, diffusion, adoption, technology, homeland security intelligence, HSINT, Department of Homeland Security, DHS, disruptive technology, technology adoption cycle, hype cycle, threats, homeland security, homeland defense, regulation, regulatory controls, domestic law enforcement, security threats, illicit appropriation

15. NUMBER OF PAGES
95

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WINDOW OF OPPORTUNITY: MITIGATING THREATS FROM DISRUPTIVE TECHNOLOGIES BEFORE WIDESPREAD ADOPTION

Christopher R. Knapp
Lieutenant, United States Navy
B.A., University of North Carolina, Chapel Hill, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2014**

Author: Christopher R. Knapp

Approved by: Rodrigo Nieto-Gómez
Thesis Advisor

Carolyn Halladay
Second Reader

Mohammad Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the pace of technology increases, so does the potential development of disruptive technology-related threats. However, by enacting proactive safety and security measures during the window of opportunity, a government can cost-effectively protect an unsuspecting and ill-prepared society before an emerging disruptive technology is widely adopted without stifling its future development.

The basis for the threat mitigation approach described herein is to inject the protective measures into the innovation cycle prior to a technology being adopted by the early majority in Everett Rogers's technology adoption cycle. This period of time (the window of opportunity) occurs when the GartnerGroup's hype cycle's trough of disillusionment aligns with Geoffrey Moore's chasm.

This thesis explores two possible courses of action for mitigating domestic security and safety threats once a new technology's window of opportunity is identified. First, domestic law enforcement can use this information to mitigate future security and safety concerns. Second, the state could design a flexible regulatory framework around the window in order to provide innovators and producers of an emerging disruptive technology with information highlighting its potential for illicit appropriation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CBRN	chemical, biological, radiological, and nuclear
DHS	Department of Homeland Security
EDT	emerging disruptive technology
eTAB	emerging technologies advisory committee
eTAC	emerging technologies assessment board
ETIPC	Emerging Technologies Interagency Policy Coordination Committee
FAA	Federal Aviation Administration
HSINT	Homeland Security Intelligence
IC	intelligence community
OTA	Office of Technology Assessment
R&D	research and development
S&T	science and technology
SCADA	supervisory control and data acquisition

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Invention is a great disturber, and it is fair to say that the greatest general cause of change in our modern civilization is invention.[1]

In 1937, the U.S. National Resources Committee Subcommittee on Technology published a report that focused on technological trends and national policy, which included the social implications of new inventions. It stated; "Most planning is not concerned with invention as such, but with the effects of inventions. These social effects come only after widespread use."[2] Despite this warning, from nearly 80 years ago, about this key attribute of how to address threats that stem from new inventions, the nation has been unable to develop and institute an effective mitigation process. This shortcoming did not occur because of limited resources or misunderstanding the innovation process; rather it occurred due to fear of inhibiting the development of new innovations.

Inventors resist the introduction of more oversight during the development phase because they fear regulation will stifle the progress of their work. Because in most cases vulnerabilities cannot be identified until the new technology is adopted by a percentage of the population, there is a significant risk involved with permitting unrestricted technological innovation because it restricts protection efforts to only a reactive approach. Therefore, if neither the government nor the companies proliferating new technologies are working to mitigate security concerns—then who is? As Kenneth Abbott writes,

> We are in the midst of one of the greatest periods of scientific and technological innovation in human history. Yet each of these technologies

---

[1] National Resources Committee, "Technological Trends and National Policy: Including the Social Implications of New Inventions," Internet Archive, accessed May 5, 2014, https://archive.org/details/technologicaltre1937unitrich.

[2] National Resources Committee, "Technological Trends and National Policy." To note, in the context of this report the term "invention" was used broadly to encompass both "invention" and "innovation." In an effort to clarify the distinction between the two terms, this thesis has adopted Joseph Schumpeter's definition of invention, "the initial development of a new idea," and innovation, "the commercially successful application of an idea." Luke Stewart, "The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review," commissioned paper for the Institute of Medicine Committee on Patient Safety and Health IT, 2010, 1, accessed February 9, 2014, http://www.iom.edu/~/media/Files/Report%20Files/2011/Health-IT/Commissioned-paper-Impact-of-Regulation-on-Innovation.pdf.

> also carries the possibility of significant risks to health, safety and the environment. And each entails other potential impacts that raise broader social, economic and ethical concerns.[3]

Practically every aspect of modern life results from advances made possible through innovation; as Nicolas Asford, Christine Ayers, and Robert Stone illustrate, "technological innovation is both a significant determinant of economic growth and important for reducing health, safety, and environmental hazards."[4] Thus, the nurturing of innovation remains of central concern to the nation's government, which is why there has been a tendency to permit innovations to develop free from control or oversight.[5] This approach cannot continue unabated. Instead, the way forward must begin with an understanding of the symbiotic relationship that exists between a technology and the society that adopts it, or in other words, accepting technological determinism and social constructionism as truisms.[6]

A. RESEARCH QUESTION

This thesis seeks to answer whether it is possible to identify threats associated with emerging disruptive innovations before these technologies are widely adopted. If so, can some form of regulatory control be used in a cost-effective manner to mitigate security concerns without stifling future innovation? As innovators develop new technologies, their focus is more on design and function than possible security and safety implications. In many cases, vulnerabilities are not identified until the technology is already adopted by a large percentage of the population. This method of introducing new

[3] The term "innovation" is used throughout this thesis to refer to the process of technology development. Gary Elvin Marchant, Kenneth W. Abbott, and Braden R. Allenby, ed. *Innovative Governance Models for Emerging Technologies* (Northampton, PA: Edward Elgar Publishing, 2013),1; Stewart, "The Impact of Regulation," 1.

[4] Nicholas Ashford, Christine Ayers and Robert Stone, "Using Regulation to Change the Market for Innovation," *Harvard Environmental Law Review* 9, no. 2 (1985): 419, http://hdl.handle.net/1721.1/1555.

[5] Stewart, "The Impact of Regulation," 1.

[6] Everett Rogers defines technological determinism as, "the belief that technology causes changes in society;" and, social constructivism as, "social factors shape a technology." Everett Rogers, *Diffusion of Innovations,* 5th ed. (New York: Free Press, 2003), 167.

technologies restricts domestic law enforcement and governmental regulatory controls to a reactive, rather than proactive, role when a disruptive technology is used with illicit intentions.

B. THESIS OVERVIEW

The preeminent concerns that the government and private sector face when attempting to identify possible future threats associated with emerging disruptive technologies (EDTs) is wasting limited time, money, and resources. While it is possible to imagine how any given emerging technology could be used illicitly, there is nothing that dictates it will ever be accepted by a large enough percentage of the population to become a meaningful threat. Therefore, before a government attempts to enact any safety or security measures it must first understand the intricacies of a technology's development, diffusion, and adoption processes. Afterward, it will then be able to identify the most cost effective period of time to enact a course of action without inhibiting an emerging technology's future progress.

The first substantive chapter of this thesis (Chapter II) will establish how EDTs pose a threat to the future of American society. Next, Chapter III will provide an in-depth explanation of innovation and technology development concepts in order to frame the context of this paper's more advanced arguments. In Chapter IV the author will demonstrate how, using the concepts explained in the preceding chapter, it is possible to identify a lull in an emerging technology's innovation and adoption cycles - the "window of opportunity."

The final two chapters (Chapters V and VI) will outline two distinctly different approaches to taking advantage of the window of opportunity in order to mitigate the security and safety threats that EDTs may pose. Chapter V will demonstrate how understanding the dynamics of this window can be utilized by domestic law enforcement (through homeland security intelligence collection, analysis, and implementation efforts), without creating a formalized regulatory framework. Alternatively, Chapter VI highlights

how designing a flexible regulatory framework around the window would provide not only a cost effective method to mitigate technology related threats, but also be perceived as helpful for a technology's future diffusion and adoption.

II. UNDERSTANDING THE THREAT

> In our haste to milk technology for immediate economic advantage, we have turned our environment into a physical and social tinderbox.[7]

As the U.S. exited the Cold War, the nation's security concerns were focused on the possibility of a "loose nuke" or a "dirty bomb." These concerns stemmed from the collapse of the Soviet Union and its loss of control over its vast stockpile of nuclear weapons. Despite the lack of proof that any Soviet nuclear material has even been smuggled into the U.S., the military and domestic law enforcement agencies have created specialized units to deal with the possibility of this threat. As an additional proactive measure, the Posse Comitatus Act was amended to allow for an exception if there was ever such an attack on U.S. soil. So why does this type of coordination and response to the illicit appropriation of nuclear material not translate to emerging technology?

The reason that the chemical, biological, radiological, and nuclear (CBRN) threat has historically been treated differently than threats that stem from EDTs is twofold. First, the general perspective that the way to protect society from a new technology can be as simple as removing its power source; and two, there has not been a large enough attack using an EDT to cause widespread concern. However, because of the ubiquity that many technologies have reached in today's society, unplugging from a diffused technology could separate society from a necessary critical infrastructure (i.e., it is no different than stating the water or power system can simply be turned off). As an example, many of the traditional U.S. critical infrastructures rely on supervisory control and data acquisition (SCADA) systems to operate, and many of them are vulnerable to a cyber-attack.[8]

In this connection, there are strong arguments to support both the threat that the cyber realm possess and that the threat is overblown and completely unrealistic. Most

---

[7] Alvin Toffler, *Future Shock* (New York: Random House, 1970), 428–29.

[8] SCADA systems allow equipment to be controlled remotely. It is commonly used to control industrial equipment for the U.S.' critical infrastructure networks.

likely, this debate over the cyber threat will continue until there is proof that a human being has been harmed as a direct result of a cyber-attack.

In order to demonstrate the complexities involved with addressing technology-related threats, this chapter will explore several different concepts. Specifically, it will investigate the historical concerns over the uninhibited development, diffusion, and adoption of technology, the difference between sustaining and disruptive technologies, the complexity of technology oversight, and the different ways that technology can be used to induce harm. Understanding the intricacies of these concepts is a necessary step toward developing an effective and practical threat mitigation plan.

A. FUTURE SHOCK

There are striking similarities between today's concerns over innovation, and those raised by futurists in the late 1970s and early 1980s. The reason for this association is because many of the futurists concerns have been partially validated by the complications the nation has experienced from the proliferation of new technologies over the past few decades. Today, these concerns are not entirely focused on fear of the unknown with respect to *how* things will change; rather, the fear stems from *how much* things will change. Even though changes from the introduction of new technology are inevitable, the manner in which a society adapts to that change can be predicated on a multitude of factors.

Schumpeter presents a linear societal and process-oriented approach to technological development, which outlines that a new innovation will go through three stages: the idea, its application, and its diffusion.[9] Referred to as the "Schumpeterian trilogy," this process establishes the basis of Alvin Toffler's concept of future shock—"the shattering stress and disorientation that we [those that diffuse a new innovation] induce in individuals by subjecting them to too much change in too short a time."[10] Toffer claims that future shock will occur if an innovation passes through the three stages

[9] Joseph Schumpeter, *Capitalism, Socialism, and Democracy* (New York: Harper, 1950).

[10] Paul Stoneman and Paul Diederen, "Technology Diffusion and Public Policy," *The Economic Journal* 104, no. 425 (1994): 918, http://www.jstor.org/stable/2234987; Toffler, *Future Shock*, 2.

quicker than a society can acclimate to it, in other words, "it is the disease of change."[11] The overall result is what Rogers calls disequilibrium, "when the rate of change is too rapid to permit the system to adjust."[12]

The pace at which new technologies are being integrated into everyday life is increasing at an exponential rate.[13] Toffler uses the typewriter to emphasize this point. The first patent for a typewriter was issued in 1714, and it took a century and a half before the machines became widely commercially available.[14] In contrast, Apple began the development of the first iPhone, called "Project Purple," in 2004, and it only took three years for the device to become commercially available. "If it takes less time to bring a new idea to the marketplace, it also takes less time for it to sweep through the society," observes Toffler.[15]

If the rate of public adoption of an emerging technology exceeds the ability of the government or private sector to institute security measures, then the public may face unforeseen and unintended threats to its safety. Furthermore, if a new technology is intentionally appropriated from the task for which it was designed and instead used criminally, the security implications become even more complex and urgent. As Toffler emphasizes:

> It is undeniably true that we frequently apply new technology stupidly and selfishly. In our haste to milk technology for immediate economic advantage, we have turned our environment into a physical and social tinderbox. Our technological powers increase, but the side effects and potential hazards also escalate.[16]

Compounding Toffler's concern is that the threat potential increases exponentially when the emerging technology is disruptive, vice sustaining, in nature.

---

[11] Toffler, *Future Shock*, 2.

[12] Rogers, *Diffusion of Innovations*, 471.

[13] Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences* (New York: Knopf, 1996), ix–xi.

[14] Toffler, *Future Shock*, 27–8.

[15] Ibid., 28.

[16] Ibid., 429.

B. SUSTAINING VERSUS DISRUPTIVE TECHNOLOGIES

Across disciplines there is a differentiation between sustaining and disruptive technologies. Clayton Christensen stipulates that all sustaining technologies "improve the performance of established products, along the dimensions of performance that mainstream customers in major markets have historically valued," (i.e., they improve established products in an established market in an expected linear manner).[17] This category of technology can progress in either an "evolutionary" or "revolutionary" fashion. The primary difference between these two terms is the amount of change from one version to the next.

In short, the progression of sustaining technologies is relatively predictable. After Apple released the iPhone 4, the next evolutionary release was the iPhone 4S. In contrast, the addition of a finger print scanner and 64-bit architecture to the iPhone 5S could be described as a revolutionary change from the iPhone 5. However, in the end despite all of the iterative changes to the iPhone, from its first generation to the most recent model, it is still a smartphone that allows an individual to make calls, text, browse the internet, and interact with third party applications. One of the benefits of sustaining technologies, as Jackie Fenn and Mark Raskio point out, is that many of these innovations, "are likely to result in longer deployment, longer learning cycles and a slower path to maturity," because they "need to be adapted to a greater degree in order to fit into existing process, culture, or technological infrastructure."[18]

Conversely, "disruptive technologies…are disruptive because they subsequently can become fully performance-competitive within the mainstream market against established products," argues Christensen.[19] Once introduced, disruptive technologies, or "competence-destroying product discontinuities" (a comparable concept conceived by

---

[17] Clayton Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Boston: Harvard Business School Press, 1997), xv, xxi; Clayton Christensen and Michael Overdorf, "Meeting the Challenge of Disruptive Change," in *Harvard Business Review on Innovation* (Boston: Harvard Business School Press, 2001), 115.

[18] Jackie Fenn and Mark Raskino, *Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time* (Boston: Harvard Business Press, 2008), 42.

[19] Christensen, *The Innovator's Dilemma*, xxiii.

Tushman and Anderson), challenge traditional industry norms and often create entirely new markets, that is, they introduce an unexpected change for which industry is not prepared.[20] In light of this distinction, disruptive technologies present a significantly more complex regulatory and security problem than their sustaining technology counterpart.

A contemporary example of a how the introduction of a new technology can change an industry is 3D printers. There are several indicators as to why 3D printers represent a disruptive technology. To begin with, the producers of 3D printers are not the same companies that have historically led the home printer market (such as Brother, Lexmark, HP, etc.). Rather, fairly new companies have entered the market that do not produce the "classic" 2D printer and instead focus only on 3D printers (such as MakerBot, Botmill, 3D Systems, etc.). Second, the traditional use of a home printer—to print word or images on some type of paper—does not translate to 3D printers. Instead, 3D printers are focused on reproducing or creating objects. Third, users of traditional printers are not able to directly translate their printer familiarity to 3D printers, and therefore these individuals will require additional training in order to operate this new technology. Fourth, while printing words or images on traditional home printers has the possibility to incite dissent and spread hate, they cannot physically cause harm to an individual (aside from inadvertent paper cut). 3D printers, however, allow individuals to effectively "print" a weapon (whether it be a gun, knife, or other dangerous object), and therefore present an entirely new security challenge that the traditional printer industry is wholly unaccustomed to addressing. This issue, as outlined by Christensen, is indicative of the lack of foresight into a developing a process to properly manage these concerns prior to the widespread introduction of a disruptive technology.[21]

---

[20] Michael Tushman and Philip Anderson, "Technological Discontinuities and Organizational Environments," *Administrative Science Quarterly* 31, no. 3 (1986): 441-44. doi: 10.2307/2392832; This concept was further expanded upon in: Michael Tushman and Charles O'Reilly, *Winning Through Innovation: A Practical Guide to Leading Organizational Change and Renewal* (Boston: Harvard Business School Press, 1997); Christensen, *The Innovator's Dilemma*, xv.

[21] Christensen and Overdorf, "Meeting the Challenge of Disruptive Change," 115.

C. MITIGATION OR PREVENTION?

"It is simply impossible to predict with any useful degree of precision how disruptive products will be used or how large their markets will be," admits Christensen.[22] Due to this uncertainty, there is no one single solution to protecting society against the illicit appropriation of an emerging disruptive technology. Currently, each of the nation's established industries employ a different type of regulatory oversight, and they all utilize different processes to protect against illicit appropriation. Therefore, each new technology that is developed will necessitate a different method of protection to ensure that the introduction of protective measures do not inadvertently inhibit the further development of the technology.

The innovation process is fluid in nature, which means that it is not possible or even useful to try and constrain or confine its parameters. As emphasized in the 1978 report on *Technological Innovation: A Critical Review of Current Knowledge*, "Exogenous elements such as human wants, social values, and the economic structure affect the nature and rate of innovation itself; for, like any creative endeavor, it arises from the interaction between individuals and the socio-cultural environment."[23] Consequently, any effort to mitigate security concerns of a new technology must begin after it is developed and it begins to integrate with society. As illustrated by Toffler, "Controls over technology need not imply limitations on the freedom to conduct research. What is at issue is not discovery but diffusion, not invention but application."[24]

For example, the introduction of personal 3D printers into an individual's home does not dictate how the device will be used. It poses no threat when it is sitting on a desk plugged into a computer—unless an individual turns it on, loads the "ink," selects a computer-aided design (CAD) file of a firearm, and selects "print." It is the human factor that creates the threat, not invention of the technology. As Jacques Ellul outlines, "There is unpredictability when in spite of every effort future events are obscure and one cannot

---

[22] Christensen, *The Innovator's Dilemma*, 154.

[23] Patrick Kelly and Melvin Kranzberg, ed., *Technological Innovation: A Critical Review of Current Knowledge* (San Francisco: San Francisco Press, 1978), ix.

[24] Toffler, *Future Shock*, 441.

give the probable course of their development. This happens often. We fail to foresee because there are so many things that we have to foresee."[25]

Because it is not possible to accurately predict how or at what rate a new technology will diffuse through a society, how a society will adapt to the technology, or how a technology will develop once it is adopted, the intention of this thesis is to address how to mitigate the new capability that the emerging technology will introduce. In agreement with a collaborative report by the Defense Threat Reduction Agency's (DTRA) Advanced Systems and Concepts Office and Science Applications International Corporation (SAIC) titled *Revolutions in Science and Technology: Future Threats to U.S. National Security*, the goal should be to "make oneself less uncomfortable" when dealing with future threats from technology, because "problems do not stand still until 'solutions' can be contrived."[26] In a similar fashion, Bertrand de Jouvenel introduced the term futuribles, whereby one would focus on objectives instead of simply assessing what is most probable.[27] This approach takes into consideration what *could* happen if we do not get involved and then it looks at what is our *desired* outcome. Effectively, the futurible concept attempts to walk the line between what is probable and what is most desirable.

For example, the intended use of a cell phone is to call another person, but during Operations Iraqi Freedom and Enduring Freedom cell phones were used as detonators for improvised explosive devices. There was no expectation that the cell phone industry could have foreseen this illicit appropriation of its technology and instituted some sort of stringent distribution regulations. Instead, the industry, as well as society, should have given some consideration to whether or not the diffusion of *cheap, disposable, and untraceable* long distance transmission devices could be illicitly appropriated, and if there was a way to mitigate this appropriation, before they were introduced.

---

[25] Jacques Ellul, *The Technological Bluff* (Grand Rapids (Mich.): W.B. Eerdmans, 1990), 82.

[26] Dallas Boyd et al., *Revolutions in Science and Technology: Future Threats to U.S. National Security*, ASCO 2011-014, Washington, DC: Defense Threat Reduction Agency, accessed February 10, 2014, 104, http://www.hsdl.org/?view&did=706488.

[27] Ellul, *The Technological Bluff*, 80.

D. THE USE OF TECHNOLOGY

Technology is neutral; it is unable to dictate whether it is used in a positive or negative manner.[28] The reason that a designer of new technology cannot entirely foresee the various uses of his or her invention is that "the lone genius in a lab or garage is an inventor, not an innovator—the invention needs to be socialized, adopted, and adapted in order to deliver value," contends Jackie Fenn and Mark Raskino.[29] Simply, in order to see the threat a technology poses, it must be used. The three categories of how the use of an EDT could pose a threat are dual-use, illicit use, and illicit appropriation.

1. Dual-Use

For the purposes of this thesis, dual-use is defined as a technology that has both a civilian and military application. For instance, GPS can be used to help an individual find his or her way around an unfamiliar city, and it can be used to guide precision munitions to their targets. Jonathan Tucker posits that the risks from dual-use technologies stem from "harm" and "misuse." He defines harm as "an inherent characteristic of a dual-use technology or material," which "encompasses a broad range of negative consequences, including fatal and nonfatal casualties, permanent disability, psychological trauma, social disruption, economic damage, and the incitement of fear."[30] Misuse, on the other hand, "is an action that violates an existing national or international statute."[31] While any technology can be misused (the most basic example is that a hammer can either be used to drive nails into wood in construction or as a weapon to inflict harm), the real concerns with misuse of a dual-use technology are those that "offer a significant qualitative or quantitative increase in destructive capacity over what is currently available."[32]

---

[28] Eduardo Calvillo Gámez and Rodrigo Nieto-Goméz, "The Case of 'Illicit Appropriation' in the Use of Technology," in *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives*, eds. Miguel Martin Vargas, Miguel A. Garcia-Ruiz, and Arthur Edwards (Hershey, PA: Information Science Reference, 2011), 211.

[29] Fenn and Raskino, *Mastering the Hype Cycle*, 38.

[30] Jonathan Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge, Mass: MIT Press, 2012), 10.

[31] Ibid.

[32] Tucker, *Innovation, Dual Use, and Security*, 3.

Even with these risks, the development of dual-use technology will (and rightfully should) continue to rise. Companies choose to pursue dual-use technologies because it is a fiscally rational course of action, and the reality is that the potential benefits that could stem from their development may very well outweigh the risks. One of the reasons that it is beneficial for a company to develop a dual-use technology is because the company will then have the opportunity to sell the end product to two types of consumers: military and civilian. With the potential to have twice the customer base, it is in a company's best fiscal interest to develop a dual-use technology. On the other hand, innovative companies face a growing "dual-use dilemma." Whereby, any attempt to mitigate risks associated with the potential misuse of a dual-use technology could adversely impact the development, and subsequent beneficial applications, of the new innovation by constraining the parameters of the technology's development or adoption.[33]

2. Illicit Use

In this thesis, illicit use of technology is defined as employing a technology in the manner in which it was designed, but for illegal purposes. A straightforward example of this would be the use of a firearm in the commission of a crime. Even though a firearm is designed for the purpose of inflicting harm and companies who produce and develop them cannot prevent an individual from using it in a criminal act, they do not endorse this type of usage. Similarly, a more widely debated example of illicit use stems from the diffusion of document scanners. Historically, if an individual were to write a book, the only manner of duplicating it without the copyrighter's consent would be through reproducing the physical book in its entirety—a tediously long and laborious process.

However, since the advent of document scanners, the book can now easily and efficiently be reproduced and then freely distributed in digital form without permission of the copyright holder. While those who invented these scanners recognized that one possible use of the technology is for an individual to replicate pages out of a book, they did not intend for the scanners to be used to violate copyright laws. Thus, the illicit use

[33] Ibid., 1.

and subsequent widespread diffusion of this technology has over time adversely effected the publishing industry as a whole.

3. Illicit Appropriation

For the purpose of this thesis, illicit appropriation of a technology is defined as using a technology for an activity that is outside the parameters of its intended use and not allowed by law. A historical example is the Brighton Hotel bombing on October 12, 1984, where the Provisional Irish Republican Army's (IRA) attempted to assassinate Margaret Thatcher at the Conservative Party's Annual Conference meeting. One month before the explosion, Patrick Magee, the bomb maker, placed Semtex in Room 629 and used a VCR as a timer for the bomb. By using a VCR timer as a long-day fuse, Magee was not only able to circumvent current security measures that were used to protect the Conservative Party, but he was also able to leave the country before his bomb detonated. As noted by Maria Rasmussen and Mohammed Hafez's workshop report on *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes, and Predictive Indicators*, "this attack entailed taking an old and tried tactic—use of explosives—and combined it with something new and original—'the most popular entertainment innovation of the 1980s, the home video recorder.'"[34]

It is safe to assume that the inventor of the video tape recorder (predecessor to the VCR), Charles Ginsburg, never intended for his technology to be used as a timer for a bomb.[35] The potential for such illicit appropriation of the technology came about as the VCR became more widespread. As Alan Dix points out,

> improvisations and adaptations around technology are not a sign of failure, things the designer forgot, but show that the technology has been

[34] Maria Rasmussen and Mohammad Hafez, *Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes and Predictive Indicators*, ASCO 2010-019, Washington, DC: Defense Threat Reduction Agency, accessed February 10, 2014, http://www.nps.edu/Academics/Centers/CCC/Research/2010%20019%20Terrorist%20Innovations%20in%20WME.pdf.

[35] *Encyclopædia Britannica*, s.v. "videocassette recorder," accessed July 15, 2014, http://www.britannica.com/EBchecked/topic/627937/videocassette-recorder; "Inventor of the Week," Lemelson-MIT, Massachusetts Institute of Technology, last modified January 2002, http://web.mit.edu/invent/iow/ginsburg.html.

> domesticated, that the users understand and are comfortable enough with the technology to use it in their own ways.[36]

The concern, of course, is users adapting the technology in a harmful way.

Rasmussen and Hafez note in their study of terrorists' use of innovations that terrorists will use any means necessary to reach their intended target, and they will seek out new innovations that may help them achieve their goal.[37] Particularly in light of the terroristic or criminal potential of new technologies, Toffler insists that those who develop new technologies also are responsible for keeping it safe.[38] However, the reason that it is unrealistic to expect that companies will make an effort to minimize misappropriation of their technology is because there are no incentives for them to do so.

In reality, there tends to only be disincentives. In order for a company to thoroughly evaluate a new technology prior to its release, it would not only have to lengthen its research and development phase, but it would also incur additional expenses. Furthermore, if it did identify the potential for illicit appropriation that rests at the core of their technology the company risks invalidating a significant portion of the work it has already done and could ultimately lose its funding. Therefore, it is much easier and less fiscally demanding for a company to simply release a product and then, if necessary, make the necessary changes in subsequent versions of their technology. As Howard Segal noted in his book *Future Imperfect: The Mixed Blessings of Technology in America*, the development of technology is being done by a "new generation" motivated purely by profit with only an allegiance to big corporations.[39]

E. CONCLUSION

Sustaining and disruptive technologies introduce different diffusion and adoption concerns, "not only are the market applications for disruptive technologies *unknown* at

---

[36] Alan Dix, "Designing for Appropriation," *Proceedings of the BCS HCI 2007 Conference, People and Computers XXI* (London, UK: BCS-eWik), 1. http://www.hcibook.com/alan/papers/HCI2007 -appropriation/.

[37] Rasmussen and Hafez, *Terrorist Innovations in Weapons of Mass Effect.*

[38] Toffler, *Future Shock*, 431–40.

[39] Howard Segal, *Future Imperfect: The Mixed Blessings of Technology in America* (Amherst: University of Massachusetts Press, 1994), 165.

the time of their development, they are *unknowable*."[40] Consequently, it is not possible to develop a singular approach that will mitigate risks associated with both types of technologies. Additionally, the enforcement of any new regulatory policies should remain as a last resort because they could inadvertently impact the innovation process in a negative way. Despite Ellul's belief that trusting inventors to not market a dangerous product is a viable method of reducing threats, all too often a technology's "harmful effects are inseparable from its beneficial effects."[41] Thus, in order to set a realistic goal, any safety or security based regulatory process must be the mitigation—not prevention—of threats from emerging technologies.

While dual-use concerns are different from those associated with the illicit appropriation of an emerging technology, they can provide a basis for understanding the complexity of future threats. For example, historically a barrier that prevented many individuals from illicitly using a dual-use technology was the need for advanced education or specialized training.[42] However, because of increased usability, automation, and collaboration this obstacle is no longer a practical prevention method for a technology related threat. In a similar fashion, an individual's capacity to illicitly appropriate an emerging technology tends to only be limited by their imagination. Without implementing an effective method of addressing the root of the threat that is enabled by technology, rather than the technology itself, the American public may continue to face new and more severe safety and security threats.

[40] Christensen, *The Innovator's Dilemma*, 143.

[41] Ellul, *The Technological Bluff*, 39, 73, 75 and 99; Toffler, *Future Shock*, 441.

[42] Tucker, *Innovation, Dual Use, and Security*, 70.

III. TECHNOLOGY DEVELOPMENT, DIFFUSION, AND ADOPTION

> If we wish technology to contribute to the achievement of our national goals and objectives, we must obtain a clearer understanding of that complex and significant activity known as the innovation process.[43]

The issue with today's proliferated technologies is that many of them "are nothing other than backbones designed to support spontaneous innovation. Millions of people potentially empowered by these backbone technologies mean millions of potential innovators all thinking and doing things that have not been thought or done before," asserts Rodrigo Nieto-Gómez.[44] In the established industry environment, there are procedures in place to oversee the development and testing of new technology before it is released to the public. The introduction of regulatory agencies like the Food and Drug Administration (FDA), National Transportation Safety Board (NTSB), Federal Communications Commission (FCC), Securities and Exchange Commission (SEC), etc. were a response to a need to protect the general public from being misled and/or harmed, and to develop and enforce a set of industry standards. In other words, these agencies act as a "filter" between the technology and society ensuring consumer protection and creating a fair trade environment.

However, EDTs present a significantly greater threat because they are not associated with a specific industry, and therefore have no defined "filter" for a technology to pass through before it is released to the public. Instead, the tendency has been to wait until the technology causes harm before an effort is made to start the lengthy process of instituting some form of oversight. This reactive approach unnecessarily puts the public at risk each time a new technology is introduced into an unregulated environment.

---

[43] Kelly and Kranzberg, *Technological Innovation*, iii.

[44] Rodrigo Nieto-Goméz, "Preventing the Next 9/10 The Homeland Security Challenges of Technological Evolution and Convergence in the Next Ten Years." *Homeland Security Affairs* 7, (2011), 2, http://hdl.handle.net/10945/24988.

Take for example the internet. The internet was originally intended to provide an efficient method for researchers to share their work, but it quickly grew into a vast network of any- and everything digital. During the advent of the internet in the 1960s, when it was known as ARPAnet, a worldwide interconnected network of computers was only a theory. However, after years of development and with support from the National Science Foundation in the 1980s, this network began to resemble the modern-day internet, albeit with one major institutional distinction: it was not available for commercial use. At this point, access to the technology was restricted to mostly the government and universities.

As the use of the internet was expanding, so was the prevalence of its vulnerabilities, which prompted Congress to pass the Computer Fraud and Abuse Act in 1986. Shortly after this legislation, in 1988, the Morris Worm was released and became the first major virus to infect the network. Acting like an internal denial-of-service attack, the worm slowed down computers to the point they were unusable. In less than three days, it had infected approximately five percent of the computers attached to the internet.[45] This attack was a clear indication of how this emerging technology was susceptible to illicit appropriation, and a contributing factor to the Defense Advanced Research Projects Agency (DARPA) creating the Computer Emergency Response Team (CERT) later that same year. The important aspect of this timeline is that it all occurred prior to the 1990s when the internet was finally commercialized.

Similar to the proliferation of all other critical infrastructures, the internet has been built for usability, efficiency, and cost effectiveness—not security—even though its architects and champions acknowledged, before its commercialization, the existence of significant threats to the security of the network. With all its known vulnerabilities—including most recently the Heartbleed Bug—the internet continues to function as a crucial part of all U.S. critical infrastructure networks.[46] Today, individuals, governments, and public and private businesses are using it on a daily basis for

[45] Peter Denning, "The Science of Computing: The Internet Worm," *American Scientist* 77, no. 2 (1989): 126–28, http://www.jstor.org/stable/27855650.

[46] Hannah Kuchler, "'Heartbleed bug' Threatens Web Traffic," *Financial Times*, April 9, 2014, http://www.ft.com/intl/cms/s/0/89c12940-bf42-11e3-a4af-00144feabdc0.html.

everything from a primary method of communication to operating SCADA systems. Due to this ubiquity, the internet has become a disruptive technology that is "too big to fail."

This section will provide an in-depth explanation on technology development, diffusion, and adoption related concepts. The purpose is to provide the necessary background information needed to conceptualize how to identify a period of time where regulatory control can be injected in a cost effective manner without inhibiting an innovation's future growth.

A. TECHNOLOGY INNOVATION PACE AND PROCESS

Technological innovation is a driving force behind the prosperity of the U.S. economy and its citizens' well-being.[47] Whether the product of publically and privately funded research and development (R&D) facilities or brainchild of the home inventor, innovation development, according to Rodgers, has six stages: recognizing a problem or need; basic and applied research; development; commercialization; diffusion and adoption; and consequences.[48] While the progression through the stages may be linear, the process is often non-directional, and each innovation can spend a different amount of time in each phase. In other words, if a problem is found during the consequences phase, the inventor can enter or re-enter the process at any stage to rectify it. Even though an innovation advances through defined stages, the process is rarely considered logical or orderly. As Geoffrey Moore writes, "[I]nnovations often need considerable experimentation and development, along with patience and tenacity, before they deliver anything worthwhile."[49] Therefore, it is very difficult to reliably assess the future success or failure of emerging technologies during the early stages of their development with any expectation of accuracy.

Especially in the case of disruptive technologies, the cost of developing a new technology often tends to outweigh its immediate benefits. A contemporary example is

[47] Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (New York: W.W. Norton & Company, 2014), 72–3; Kelly and Kranzberg, *Technological Innovation*, iii.

[48] Rogers, *Diffusion of Innovations*, 137–57.

[49] Fenn and Raskino, *Mastering the Hype Cycle*, 9.

the Navy's efforts to develop F/A-18 Hornets that use alternative jet fuel made from algae.[50] The Navy paid up to $150 per gallon for the algae-based fuel, at a time when conventional jet fuel only cost $2.88 a gallon.[51] The difference in the two prices owes to the cost of development; however, if the new fuel becomes ubiquitous the cost per gallon will decrease dramatically as the production process is refined.

The success of alternative fuel, along with many other innovations, tends to be directly linked to the pace of its development and, ultimately, its rate of adoption. Many prominent innovation scholars, including Everett Rogers and Alvin Toffler, agree that the pace of technological innovation is increasing at an exponential rate.[52] Take, for example, the $35 million-dollar Cray-2 supercomputer that was unveiled in 1985 and Apple's $499 iPad 2 tablet computer that was released in 2011. While both of these computers boast identical calculation speeds, the iPad was not only portable, but it also included a slew of additional technologies, including "a GPS receiver, digital compass, accelerometer, gyroscope, and light sensor."[53] A major factor in this escalation in innovation is the availability of rapid experimentation sources and methods, which have become readily accessible to inventors. Through the use of refined, standardized, and modernized resources, inventors are able to reduce the cost of failures inherent in the innovation process. Specifically, the use of "computer simulation, rapid prototyping, and combinatorial chemistry" allows an increased number of inventors to get more out of their sometimes limited resources and funding.[54] No less a figure than Thomas Edison believed that "rapid and frequent experimentation" leads to "great innovation."

---

[50] The F/A-18 Hornet is the Navy's carrier-based multi-role fighter aircraft capable of air-to-air and air-to-ground combat.

[51] Lachlan Markay, "Pentagon Paid $150 per Gallon for Green Jet Fuel: Report," *The Washington Times*, May 7, 2014, http://www.washingtontimes.com/.

[52] Rogers, *Diffusion of Innovations*; Toffler, *Future Shock*, 428–29.

[53] The cost of the Cray-2 supercomputer is adjusted to 2011 dollars; Brynjolfsson and McAfee, *The Second Machine Age*, 49–51.

[54] Stefan Thomke, "Enlightened Experimentation: The New Imperative for Innovation," *Harvard Business Review* 79, no. 2 (2001): 181. Reprinted in *Harvard Business Review on Innovation*. Boston, MA: Harvard Business School Press, 2001.

While some academics—for example, Stefan Thomke—focus on the physical attributes that enable rapid innovation (computer simulation, rapid prototyping, and combinatorial chemistry), Rogers and Toffler centered their work on investigating how innovations propagate through a society and the effects this *diffusion* has on the populace.[55] What this scholar and futurist ultimately concluded was that even if there is a recognizable structure to the diffusion of an emerging innovation, the process may still yield unexpected results.[56]

Take, for example, the progression of smaller and more powerful cellphones. While this technology progressed over the years in a relatively controlled and predictable fashion, it has caused a cultural shift among innovators and consumers. Originally, cellphones were used only as a method of wireless voice communication between two parties, but today most individuals rarely use them to make phone calls. This evolutionary shift is so widespread that cellphone development companies' advertisements seldom promote call quality as a selling point for their products. As Elting Morison describes in his book, *Me, Machines, and Modern Times*, the current focus in innovation development is on continually trying to attain new and better capabilities, rather than attempting to get the most out of the technology that already exists.[57] While this approach may be financially beneficial to an inventor it continually introduces unfamiliar and unrefined technologies into society.

Technological change has brought about a dramatic increase in not only the rate of development of new innovations, but also society's *rate of adoption*.[58] The preeminent concerns that the government and private sector face when attempting to identify possible future threats associated with EDTs is wasting limited time, money, and resources. While it is theoretically possible to imagine how any given emerging technology could be used

---

[55] Rogers stipulates that diffusion is specifically associated with "new ideas" that can elicit "social change" ultimately affecting societal norms; Thomke, "Enlightened Experimentation," 181; Rogers, *Diffusion of Innovations*, 5–6; Toffler, *Future Shock*, 428–29.

[56] Rogers, *Diffusion of Innovations*, 6.

[57] Elting Morison, *Men, Machines, and Modern Times* (Cambridge, MA: M.I.T. Press, 1966), 214.

[58] "Rate of adoption is the relative speed with which an innovation is adopted by members of a social system." Rogers, *Diffusion of Innovations*, 23, 221.

in an illicit manner, there is nothing that dictates that type of use will ever be accepted by a large enough percentage of the population to become a meaningful threat. Therefore, the effectiveness of an EDT threat assessment hinges on an in-depth understanding of the technology adoption process.

B. TECHNOLOGY ADOPTION CYCLE

Supported by his observations and a review of empirical research, Rogers identifies five categories of technology adopters: innovators, early adopters, early majority, late majority, and laggards (as illustrated in Figure 1).

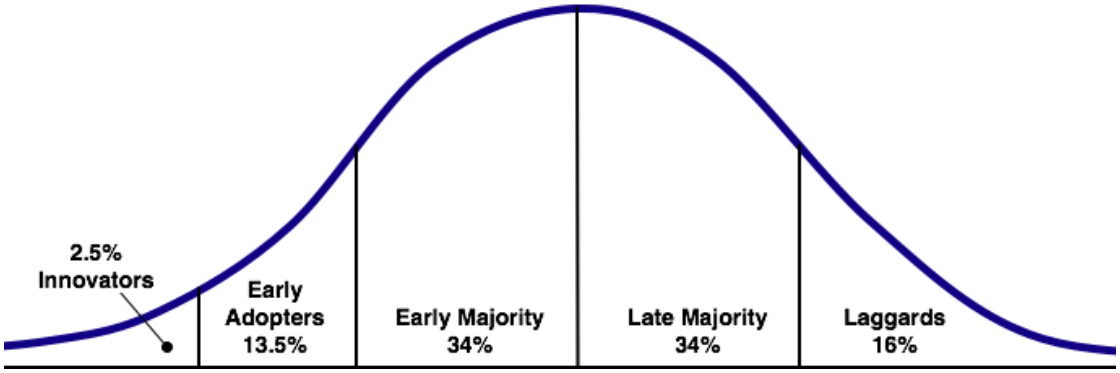

Figure 1. Technology Adoption Cycle[59]

These categories are based on "ideal types," which is a categorization methodology linked to how an individual's intrinsic values will affect their adoption of a new technology.[60] Rogers correctly acknowledges that, regardless of the designed use or purpose of a technology, individuals' "psychological and social profiles" will affect the point at which they will adopt a new technology.[61] Effectively, his research demonstrates that as an innovation progresses toward mainstream acceptance, it will go through a fairly predictable adoption cycle.[62] The basis of how a regulatory group will identify the

[59] Rogers, *Diffusion of Innovations*, 280–2.

[60] Ibid., 282.

[61] Geoffrey Moore, *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers* (New York: HarperBusiness, 1999), 13.

[62] Rogers, *Diffusion of Innovations*, 22 and 279–85.

appropriate time to attempt some form of EDT threat mitigation rests on their understanding of the characteristics that make up each adoption group, especially the differences between the early adopters and the early majority.

1. Innovators

The first and smallest adoption category (2.5 percent) is the innovators. These are the individuals in a society who are continuously seeking out and applying new ideas and technology as soon as they become available. Motivated by the need always to be the first to incorporate a new technology, innovators must rely on their own judgment and technical abilities to determine how to integrate the new innovation. Therefore, they are willing to accept substantial risk of failure and setbacks during their adoption process. One of the most important roles that innovators serve is as "gatekeeper" between inventors and end users (consumers) of a new innovation. An innovator's acceptance of a new technology can effectively begin, or quickly end, the diffusion process.[63]

2. Early Adopters

The next category in the technology adoption cycle is the early adopters. Even though these individuals comprise the second-smallest category (13.5 percent), their opinions of a new technology are extremely important to the overall diffusion process. As Rogers stipulates, the early adopter's "stamp of approval" is how this adopter category manages to "decrease uncertainty about a new idea," which enables a technology's continued diffusion.[64] Additionally, they are intricately involved with change agents and have substantial influence over whether or not a technology will reach critical mass.[65] Early adopters are continually seeking out new technologies and they understand that an emerging innovation may fail to meet all stated expectations. If innovators are the

---

[63] Rogers, *Diffusion of Innovations*, 22 and 282–83.

[64] Ibid.

[65] Critical mass is the point at which a population's adoption of an innovation becomes self-sustaining. A change agent is an individual or group that works to "influence clients' innovation-decisions" by providing a "communication link between a resource system with some kind of expertise and client system." Both of these concepts will be explained in detail in later sections. Thomas Schelling, *Micromotives and Macrobehavior* (New York: Norton, 1978), 91–6; Rogers, *Diffusion of Innovations*, 366 and 368.

gatekeepers who allow a technology to move from the lab to the public, the early adopters serve as the pathway toward mainstream acceptance.

3. Early Majority

As the early majority adopts a technology, the adoption rate moves toward its highest point on the bell-curve–shaped technology adoption cycle. Made up of followers, rather than leaders, the early majority forms one of the two largest categories of the technology adoption cycle. Totaling 34 percent of a society's technology adopters, the early majority is, in Rogers's description, "deliberate" in its actions. He indicates that while the early majority is willing to accept a new technology, these individuals will only do so if they can identify a specific and beneficial use for it. In other words, the early majority's motivation for technology adoption is driven more by "needs," rather than "wants." Therefore, even though this group approves of the benefits that can be had from technological advances, it has minimal patience for technology that fails to meet their expectations.[66]

4. Late Majority

The late majority also makes up one third of the adoption. However, it differs markedly from the early majority in that this group is "skeptical" of adopting a new technology until it is a proven commodity. This group looks to the preceding adoption groups to demonstrate the benefits of the technology before it is willing to accept the innovation. Additionally, it is necessary to remove the safety and security risks before this group will begin to integrate the new technology into its established system.[67]

5. Laggards

Finally, the last adoption category comprises the laggards. This group accounts for the trailing 16 percent of the social system that adopts a technology. For laggards, the decision to adopt is not simply based on proving that the new technology is beneficial;

---

[66] Rogers, *Diffusion of Innovations*, 22 and 283.

[67] Ibid., 22 and 284.

instead laggards need to be shown the deficiencies in the technology they are currently using. In other words laggards "must be certain that a new idea will not fail before they can adopt."[68]

C. STRATEGIC INFLECTION POINT, DOMINANT DESIGN, AND CRITICAL MASS

Often as technologies propagate through a society they reach a point at which they either become accepted by the masses or simply slip into oblivion. This section will highlight three concepts—strategic inflection point, dominant design, and critical mass – that can help a regulatory group identify which technologies have the best chance at progressing toward ubiquity.

1. Strategic Inflection Point

The strategic inflection point is used to signify a definitive change from the old to the new or the negative to the positive.[69] Figure 2 shows that when a business reaches an inflection point, its future growth will either improve or decline.

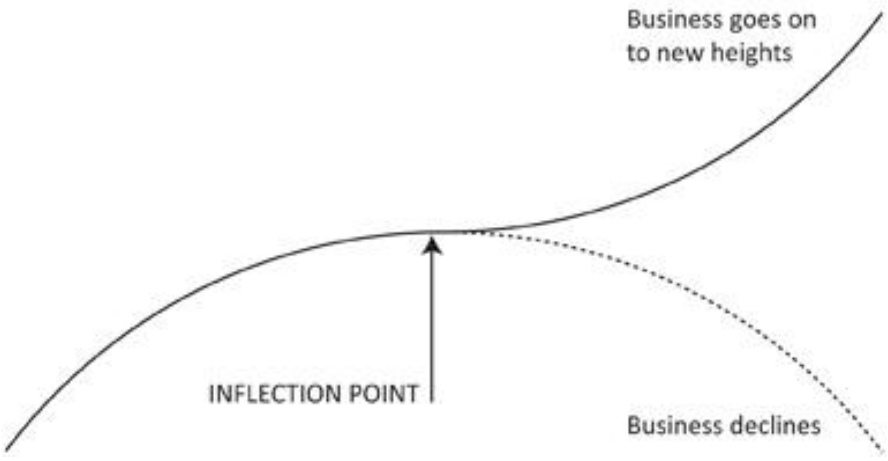

Figure 2. Strategic Inflection Point[70]

[68] Rogers, *Diffusion of Innovations*, 22 and 284–85.

[69] Andrew Grove, *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career* (New York: Currency Doubleday, 1996), 33.

[70] Ibid., 32.

On the macro level, Andrew Grove claims that in most situations, it is nearly impossible to tell the specific moment when a strategic inflection point occurs. However, Brynjolfsson and McAfee argue that the United States is currently in the middle of a profoundly significant inflection point—what they call the "second machine age." Based on Moore's Law, Brynjolfsson and McAfee claim that over the next quarter-century, computing power will increase "over a thousand-fold," pushing society toward "the creation of true machine intelligence and the connection of all humans via a common digital network."[71] For society to increase its chances for a positive improvement after it passes this inflection point, its first step is to recognize and accept the changes that are occurring so that it can facilitate the new innovation's widespread diffusion and adoption.[72]

2. Dominant Design

At more of a micro level, the implications of failing to recognize when an inflection point occurs are evident in how a dominant design emerges. In situations where competing innovations are vying for a market that is only able to sustain one design, the strategic inflection point represents the point at which one design succeeds and the other fails.[73] Examples are the introduction of videocassette magnetic tape recording devices (Betamax in 1975 and VHS in 1976) and high-definition optical disc storage formats (both Blu-ray and HD-DVD were released in the United States during 2006). One of these technologies was destined to become the nation's standard, but the driving force behind that decision was not based on the innovation that was technologically superior; rather, the deciding factors were its adoption by correlative industries and the product's marketing efforts. James Utterback and William Abernathy, who coined the term dominant design, also posit that once a dominant design is widely accepted, it will remain

[71] Gordon E. Moore argues that computing power doubles every two years. This argument is known as Moore's Law; Brynjolfsson and McAfee, *The Second Machine Age*, 251.

[72] While Andrew Grove states in his book, *Only the Paranoid Survive*, that the strategic inflection point signifies a transitional moment in the life of a company, for the purposes of this thesis the concept has been appropriated to indicate the point at which a technology will be accepted or rejected by mainstream society.

[73] James Utterback and William Abernathy, "A Dynamic Model of Product and Process Innovation," *Omega* 3, no. 6 (1975): 639–56, doi: 10.1016/0305-0483(75)90068-7.

the predominant choice until a new disruptive innovation restarts the process (in this case, VHS was not ousted until DVDs became the new standard).[74]

3. Critical Mass

Influenced by the technology adoption cycle concept, Frank Bass set out to develop a mathematical formula that try and predict the rate of adoption.[75] Built with a nonlinear differential equation the Bass forecasting model "seeks to forecast how many adoptions of a new product will occur at future time periods."[76] While a considerable number of sources state that the model has been widely adopted and that it is still in use, there is not much empirical evidence that substantiates its effectiveness. However, what the Bass forecasting model attempts to predict is the point at which an innovation reaches *critical mass*.

During the adoption process of a new technology, Thomas Schelling theorizes there is a point at which a population's adoption of an innovation becomes self-sustaining.[77] Termed "critical mass," it begins when early adopters embrace an innovation.[78] Once a technology moves passed a strategic inflection point its adoption may either progress gradually, or, if it achieves critical mass, it can be propelled forward. Figure 3 illustrates that, based on the site's number of users, Facebook's adoption reached critical mass around 2007.

---

[74] Utterback and Abernathy, "A Dynamic Model of Product and Process Innovation," 639–56; Later it was also supported by: James Utterback, and Linsu Kim; Philip Anderson and Michael Tushman, "Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change," *Administrative Science Quarterly* 35, no. 4 (1990): 604–633, doi: 10.2307/2393511; James Utterback and Linsu Kim, "Invasion of a Stable Business by Radical Innovation," in *The Management of Productivity and Technology in Manufacturing*, ed. Paul Kleindorfer (New York: Plenum Press, 1985): 113–51, http://dx.doi.org/10.1007/978-1-4613-2507-9_5.

[75] "The Origin of the Bass Model," Bass's Basement Research Institute, accessed March 11, 2014, http://www.bassbasement.org/BassModel/Default.aspx.

[76] Rogers, *Diffusion of Innovations*, 208–13. It is also commonly referred to as the "Bass model" and the "Bass diffusion model."

[77] Schelling, *Micromotives and Macrobehavior*, 91–6; Rogers, *Diffusion of Innovations*, 343 and 363.

[78] Ibid., 283.

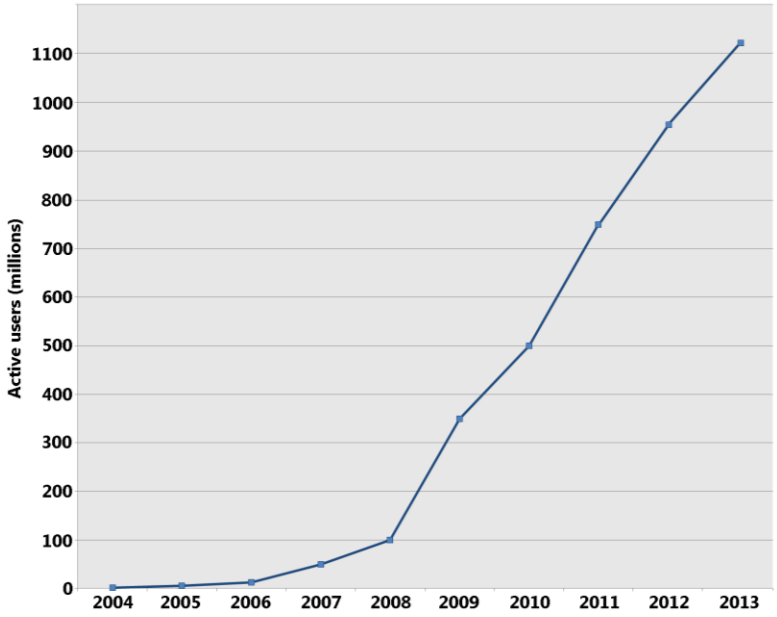

Figure 3. Number of Facebook users from 2004–2013[79]

D. THE CHASM

In order for the momentum from a technology reaching critical mass to carry it through to the next adoption category, the early majority, the technology must first cross the "chasm." Geoffrey Moore proposes the chasm concept as a divide that exists between the early adopters and the early majority. Figure 4 shows the chasm, as Moore describes it.

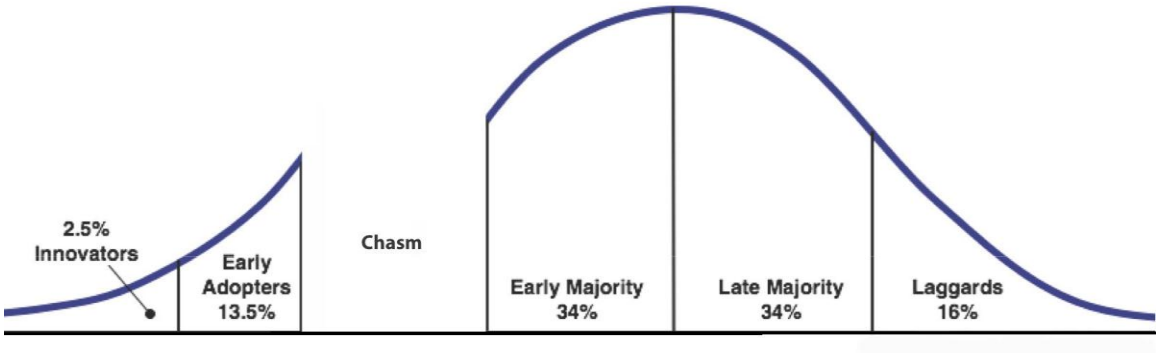

Figure 4. The Chasm[80]

[79] "Facebook," Wikipedia, accessed June 13, 2014, http://en.wikipedia.org/wiki/Facebook.

According to Moore, "the chasm represents the gulf between two distinct marketplaces for technology productions-the first, an early market dominated by early adopters and insiders who are quick to appreciate the nature and benefits of the new development, and the second a mainstream market representing 'the rest of us,' people who want the benefits of new technology but who do not want to 'experience' it in all its gory details."[81] Despite pointing out that there is no research available that fully supports Moore's chasm theory, Rogers does indicate that there are "important differences between" adopter categories.[82]

Moore insists that when attempting to guide a new technology through the adoption cycle marketers must navigate the transition between the foresight of the first adopters and the pragmatism of the mainstream market segments, and the most challenging division exists between the early adopters and early majority.[83] Effectively, the movement between these two groups requires a marketing shift whereby the focus transitions from the technology to the market that is adopting it. Even though the chasm theory is a marketing concept, it properly signifies not only the importance of understanding the different characteristics of the adoption groups, but it also highlights a point in the adoption cycle where a distributor of an emerging technology would be most likely to heed external input.[84]

E. THE HYPE CYCLE

The last concept utilized in this thesis is used to further one's understanding of the complexities of not only technological development, but also technological interest—the GartnerGroup's hype cycle. The GartnerGroup is a private company that has built a business around understanding the development of emerging technologies. In an effort to

---

[80] This graph was originally based on Rogers's Technology Adoption Cycle, and has been modified to reflect Moore's Chasm. Rogers, *Diffusion of Innovations*, 280–2; Moore, *Crossing the Chasm*, 17.

[81] Moore, *Crossing the Chasm*, xiv.

[82] Rogers, *Diffusion of Innovations*, 282.

[83] Moore, *Crossing the Chasm*, 19 and 52–3.

[84] Ibid., 199.

demonstrate that a lifecycle exists for new technologies it developed the "hype cycle."[85] This decision aid annually outlines current emerging technologies, and for snapshot in time, where they are in their development and adoption process.[86] However, because technologies are not always developed and then adopted in a linear fashion (for example, the precursor to the modern day fax machine was invented in 1924, but was not widely adopted until the late 1980s), the GarterGroup states that the hype cycle does not attempt to predict the future of any of the listed technologies. In other words, just because a technology is show to be building momentum in 2014, that does not mean that in 2015 it will continue to progress through the cycle.[87]

There are five stages to the hype cycle: the innovation trigger, peak of inflated expectations, trough of disillusionment, slope of enlightenment, and plateau of productivity.[88] As demonstrated in Figure 5, each stage is used to represent the critical junctures of a technology's development and diffusion life cycle.

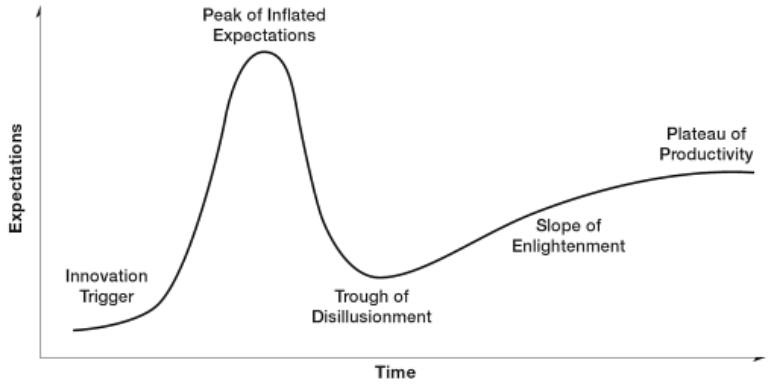

Figure 5. GartnerGroup's Hype Cycle[89]

[85] Jackie Fenn and Mark Raskino, "Gartner's Hype Cycle Special Report for 2013," Gartner Insight, Gartner, Inc., accessed February 11, 2014, http://my.gartner.com/portal/server.pt?open=512&objID =256&mode=2&PageID=2350940&resId=2574916.

[86] Fenn and Raskino, "Gartner's Hype Cycle Special Report for 2013."

[87] Ibid.

[88] An extended version of the hype cycle exists that includes two additional stages: the swamp of diminishing returns and cliff of obsolescence.

[89] Fenn and Raskino, *Mastering the Hype Cycle*, 9.

Overall, the hype cycle seeks to visually represent the "interplay of two factors: human nature and the nature of innovation."[90] Even though the development of new innovations has historically been aligned with human nature (i.e., humans would invent a technology for a defined purpose), modern technological advances have managed to push these two factors "out of sync" with one another.[91] This progression has reached a point where, "technological progress and social progress…often conflict."[92]

The hype cycle begins with the innovation trigger, which is the event that first introduces the technology to a society. In many cases this occurs with the release of a beta version of the technology. As the "hype" in the technology begins to build the interest in the technology progresses toward the peak of inflated expectations. A technology is effectively pushed toward this "peak" by media hype and "a bandwagon effect."[93] However, when the technology fails to meet all of the expectations set before it, or problems with its development arise, it starts to slide into the trough of disillusionment where a technology could remain for a substantial period of time if there is nothing to push or pull it to the next stage of the cycle. A causal factor for this stagnation is the lack of public interest in continued development that leads to a stalled rate of adoption.

While in the trough, many innovations go through considerable changes in order to climb the slope of enlightenment. A major contributing factor that facilitates a technology's continued progression through the cycle is, "drawing on the experience of early adopters," whereby "understanding grows about where the innovation can be used to good effect," states Fenn and Raskino.[94] Once a technology summits the slope, it enters into the plateau of productivity. Represented by stable and refined product releases that mitigate adoption risks, the plateau is where widespread adoption begins and profitability from the technology is possible.[95]

---

[90] Ibid., 25.

[91] Fenn and Raskino, *Mastering the Hype Cycle*, 25.

[92] Segal, *Future Imperfect*, 200.

[93] Fenn and Raskino, *Mastering the Hype Cycle*, 8.

[94] Ibid., 10.

[95] Ibid., 8–10.

F. CONCLUSION

Despite decades of modern innovation development and discussions about the inherent risks with widespread adoption of many emerging technologies, there are still those in today's society that, like Segal, believe modern technology, "remains ill-defined, poorly conceived, and misunderstood by many."[96] However, this is a self-induced and self-perpetuated problem that does not require a complex or convoluted solution. In fact, New Order Amish have, since their formation in the 1960s, understood that the integration of a technology into their community will introduce unknown and unexpected changes.[97] Unlike the Old Order Amish, the New Order does not wholly ignore technological advances, instead "they seek those aspects of an innovation that support the lives they want, and avoid those aspects that weaken or detract from such lives."[98] While their technology assessment process can be fairly lengthy, the lesson that mainstream society needs to learn from this small sect of individuals is that, "nothing actually compels us to adopt every new technology and embrace every new idea."[99]

The concepts described in this chapter intend to provide the necessary background material needed to understand the intricacies of technology innovation, diffusion, and adoption. For years futurists, like Toffler, have tried to warn society about the risks that are inherent in its historical "adopt and see" approach to evaluating emerging technologies. In order to heed their warnings, and adopt a more proactive approach to technology related threat mitigation efforts, society must use the complexities inherent in technology development to their advantage. Specifically, regulatory or threat mitigation efforts must be enacted during the period of time where there is a lull in the innovation processes.

---

[96] Segal, *Future Imperfect*, xii.

[97] Fenn and Raskino, *Mastering the Hype Cycle*, 92.

[98] Ibid.

[99] Ibid.

IV. IDENTIFYING THE WINDOW

> Though the influence of invention may be so great as to be immeasurable, as in the case of gunpowder or the printing press, there is usually opportunity to anticipate its impact upon society *since it never comes instantaneously without signals*. For invention is a process and there are faint beginnings, development, diffusion, and social influences, occurring in sequence.[100]

Due to the complexities of integrating disruptive technologies into the nation's industry and culture, the government and the private sector have chosen to adopt a "wait and see" approach to addressing threats that stem from the introduction of disruptive technologies. In other words, any effort made to protect against threats from a new technology are often limited until misuse or criminality presents a constant threat to the American public. While it is important for government and industry to acknowledge that trying to regulate or police all emerging technologies is fiscally irresponsible and socially unacceptable, they also may not simply stand idly by while individual citizens and private businesses are forced to protect themselves from newly developed emerging threats.

The first step toward developing a method of mitigating threats from EDTs is acknowledging that the nation is on the cusp of entering Brynjolfsson and McAfee's second machine age. The evidence of this strategic inflection point manifests itself through the increased pace of innovation development, sources and methods of technology diffusion, and the subsequent changes in industry that result. "Many technologies that used to be found only in science fiction are becoming everyday reality," the authors write, and with these additions society is facing "difficult challenges and choices."[101] There is no reason to fear the second machine age because it is a change that represents progress; rather, society should proceed with a cautious optimism toward the integration of new and unproven technologies.

Through an in-depth understanding of the innovation development, adoption, and diffusion process, it is possible to identify a window of opportunity where the

---

[100] National Resources Committee, "Technological Trends and National Policy," ix.

[101] Brynjolfsson and McAfee, *The Second Machine Age*, 11 and 34.

introduction of proactive security measures would have the best chance of mitigating the development of future threats.[102] This window exists where a new technology falls into the chasm that occurs as it transitions from the early adopters to early majority in Rogers's technology adoption cycle; it also appears when the technology slides into the hype cycle's trough of disillusionment. In order for a disruptive technology to cross the chasm and climb out of the trough, it must meet the needs of the follow on adoption groups as it secures itself as a viable innovation. Thus, this alignment of the chasm and the trough create a window of opportunity where technology developers, producers, and distributors are receptive and appreciative of external input.

Tucker points that the life of a disruptive technology begins in one of four places that conduct R&D: "private industry, government research laboratories, universities or nonprofit research institutes, and entities outside a formal institutional context," (i.e., the at home inventor).[103] The dynamic nature of the innovation development process, combined with the fluidity of these R&D environments, precludes identifying security and safety concerns prior to the innovation trigger. "In spite of popular stereotypes to the contrary, an innovation doesn't spring fully formed from the mind of the inventor and into the hands of the user. It needs a period of time to diffuse in markets," where its real purpose and usefulness can be discovered.[104] Therefore, the starting point for an evaluation of an emerging disruptive innovation begins with the innovators and their recognition of the innovation trigger.

"Innovations can have an extremely long research and development preamble before they reach a meaningful trigger point, including several false starts with minor peaks and troughs," contend Fenn and Raskino.[105] It takes the actions and involvement of the innovators—and their "venturesome" nature—to detect and approve when an innovation trigger occurs and it is time to initiate the start of the diffusion process. Alternatively, in some cases, the innovators' investigation into the possible uses of a new

[102] Tushman, *Winning Through Innovation*, 160.

[103] Tucker, *Innovation, Dual Use, and Security*, 76.

[104] Fenn and Raskino, *Mastering the Hype Cycle*, 35.

[105] Ibid., 69.

technology can produce an innovation trigger. In either case, it is the innovator's influence that begins to push a new technology through the beginning of the hype cycle toward the peak of inflated expectations.

A. UNDERSTANDING EARLY ADOPTERS

If the innovators push the technology toward the peak, then the early adopters are the ones who pull it the rest of the way up. As Rogers writes, "Earlier Adopters have greater empathy, less dogmatism, a greater ability to deal with abstractions, greater rationality, greater intelligence, a more favorable attitude toward change, a greater ability to cope with uncertainty and risk, a more favorable attitude toward science, less fatalism and greater self-efficacy," when compared to their later-adopter counterparts.[106] As demonstrated in a wide range of different fields of innovation, the involvement of the early adopter category is an important step toward a technology's continued diffusion.[107] In many ways this group's approval and acceptance of a new technology can serve as an indispensable filter—or the voice of reason—between the risk-taking innovators and the more conservative later adopters.

As the technology progresses toward the peak, it approaches its first strategic inflection point. Due to the infancy of the technology and the limited scope of its adoption, it is highly susceptible to social contagion—otherwise known as the bandwagon effect.[108] Therefore, the positive or negative direction of this phenomenon may push the technology toward a higher peak, or start its slide into the trough of disillusionment. Even if the technology is able to progress to a higher peak of inflated expectations, when its momentum subsides it will begin to slide into the trough. One of the situations that can interrupt the diffusion of a technology, and curb its momentum, is the transition from the early adopters to the early majority (i.e., when a technology attempts to cross the chasm).

---

[106] Rogers, *Diffusion of Innovations*, 298.

[107] Nicholas Ashford, ed., *National Support for Science & Technology: An Examination of Foreign Experience* (Cambridge: MIT Press, 1975), I-20.

[108] Fenn and Raskino, *Mastering the Hype Cycle*, 29.

B. THE CHASM AND TROUGH

As a new technology attempts to cross the chasm it slides into the trough of disillusionment. This situation produces a lull in both the technology adoption and hype cycles (as illustrated in Figure 6) where, if embraced, a new technology could be evaluated for safety and security considerations without impacting its further diffusion.

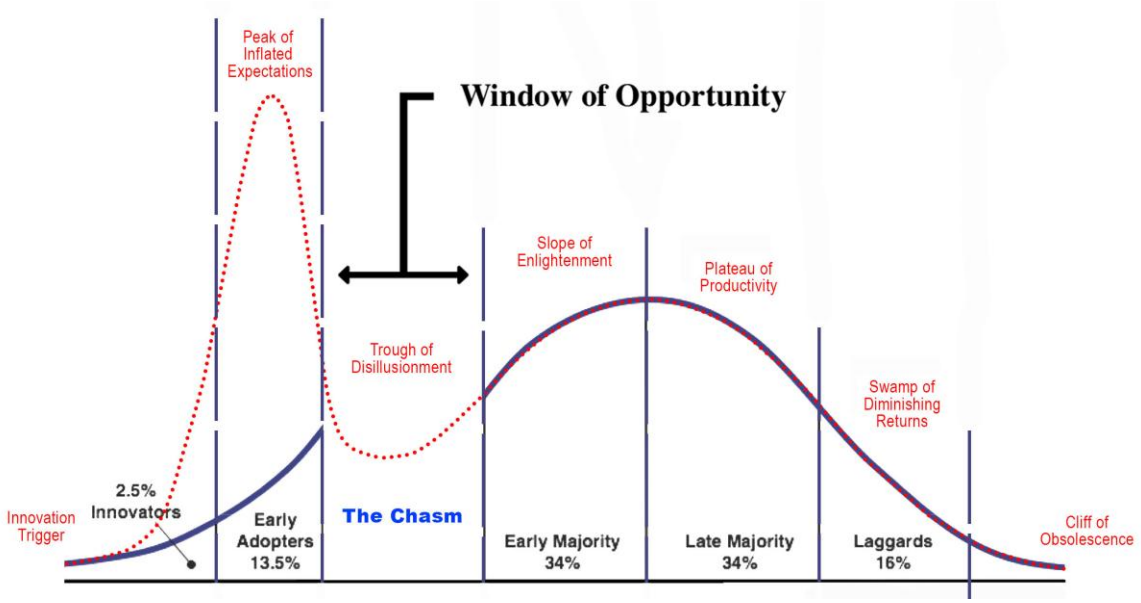

Figure 6. The Window of Opportunity[109]

As Gregory Mandel notes, it is possible to turn the uncertainty that is created by the complexities that surround understanding disruptive technologies into an advantage. Technology investors, developers, producers, distributors, regulators, and adopters are all faced with "common concerns" as the technology remains in the trough/chasm.[110] Mandel asserts that this situation "present[s] a unique opportunity to bring together diverse stakeholders to produce a collaborative…process rather than a resource-draining adversarial battle," because "interests and organizations have not yet strongly vested

[109] The figure identifies the parallels between the Technology Adoption Cycle, the Chasm, and the Hype Cycle. It was designed by the author, and based on Rogers's Technology Adoption Cycle, Moore's Chasm, and GartnerGroup's Hype Cycle. Rogers, *Diffusion of Innovations*, 280–2; Moore, *Crossing the Chasm*, 17; Fenn and Raskino, *Mastering the Hype Cycle*, 9.

[110] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 45 and 50; Fenn and Raskino, *Mastering the Hype Cycle*, 95–6.

around a particular system or status quo."[111] In other words, all of the involved parties want to see the technology climb out of the trough/chasm, and are willing to work together to make it happen—even if it involves modifying the technology.[112]

A transition from a technology-centric to a market-centric focus is required in order to cross the chasm.[113] Innovators and early adopters view technology adoption as a necessary part of life, and their interest in an emerging technology is heavily influenced by a desire of acquiring something that is state-of-the-art. Conversely, the early majority, late majority, and laggards, are more skeptical about adoption, and must be shown the potential benefits the technology could provide before they will accept it. Overall, the early majority, late majority, and laggards have substantially different goals and motivations than the innovators and early adopters. In an unregulated environment, like the one that surrounds EDTs, "early adopters are the guinea pigs that get hit with the problems and risks of an immature innovation," as the mainstream adoption groups sit on the sidelines waiting to see the real-world viability of the technology.[114] A significant contributor to reducing the adoption risk for later adopters is the mitigation of safety and security concerns.[115] The benefit of having an adoption group focused on these public interest areas, Mandel stipulates, is that they commonly receive "widespread support."[116] Additionally, by addressing these concerns early in the adoption process it not only provides an opportunity to institute controls to mitigate the future illicit use of a disruptive technology, but it also has the potential to help enable its future widespread diffusion.[117]

Taking a lesson from the issues faced by mitigating the dual-use concerns in the biotechnology field, Mandel and Gerald Epstein assert that, "intervention at an early

---

[111] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 45 and 51.

[112] Ibid., 51.

[113] Christensen, *The Innovator's Dilemma*, xxvi.

[114] Fenn and Raskino, *Mastering the Hype Cycle*, 12, 13, 37 and 63.

[115] Rogers, *Diffusion of Innovations*, 241 and 249.

[116] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 51–2.

[117] Christensen, *The Innovator's Dilemma*, xxvi.

stage is…problematic because political interest is low and little is known about the risks and benefits of the technology."[118] Before an innovation falls into the trough of disillusionment, information about the disruptive technology is widely disseminated in order to build up the hype. However, when an innovation is in the trough, a large percentage of population is still trying to make up its mind about the technology's future viability.[119] Therefore, at the bottom of the trough, another strategic inflection point exists.

Even though the trough provides an opportunity for a second generation of the technology to be released, along with a shift in marketing to focus on mainstream adopters, industry leaders often face significant challenges in initiating the requisite changes. These challenges occur because, as Grove points out, "the more successful a participant was in the old industry structure, the more threatened it is by the change and the more reluctant it is to adapt to it."[120] However, by uniting around the aforementioned uncertainty that exists at this transitional juncture it is possible for a technology to be pushed out of the chasm and up the slope of enlightenment by facing head on the adoption concerns of the early majority.

C. ACHIEVING WIDESPREAD ADOPTION

In 1970, economist Edwin Mansfield demonstrated the inherent diffusion benefits to educating users about a technology prior to their adoption.[121] Because the early majority are not considered leaders and have no vested interest in a disruptive technology's future diffusion, their real contribution is the manner in which they "provide interconnectedness in the system's interpersonal networks."[122] However, this characteristic can either be an advantage or disadvantage to a diffusing technology. If the early majority does not approve of the technology's benefits and begin adopting it en masse, the technology may not make it very far up the slope (and completely out of the

[118] Tucker, *Innovation, Dual Use, and Security*, 36.

[119] Ibid.

[120] Grove, *Only the Paranoid Survive*, 50–1.

[121] Kelly and Kranzberg, *Technological Innovation*, xi.

[122] Rogers, *Diffusion of Innovations*, 283–84.

chasm) before it stagnates. Conversely, by learning and adapting an innovation based on feedback from the innovator's and early adopter's value networks, it is possible for those marketing the technology to harness the "deliberate" nature of the early majority to help the technology diffuse into the late majority.[123]

Disruptive technologies have a tendency to fail if they are introduced before end users actually need or want them.[124] Therefore, it is not possible to force the adoption of a new technology on later adopters without educating them on its value adding benefits. This education can be accomplished by creating a support system that makes the technology more user friendly and lowers adoption risks.[125] With the ultimate goal of achieving critical mass, a technology's progression up the slope of enlightenment is directly related to mitigating the early majority's adoption hurdles. Often, as a technology "matures from an uncertain value proposition with high risk of failure to a predictable value proposition with low risk…it goes mainstream."[126] Once established on the slope, the transition to the plateau of productivity and the later adoption groups (late majority and laggards) becomes dependent on whether or not the focus can remain on the needs of the technology's market, rather than the technology itself.

In the plateau, "most of the problems and unknowns have been ironed out of the innovation by earlier adopters, and the cost and functionality of products have stabilized."[127] Once this stabilization occurs, a market and/or industry will begin to form around the disruptive technology, and pull it toward full maturity and societal integration.[128] Additionally, "the hype around it typically disappears and is replaced by a solid body of knowledge."[129] The primary concerns for the technology's future are now

---

[123] Rogers, *Diffusion of Innovations*, 283–84; Christensen, *The Innovator's Dilemma*, 32; Peter Coughlan, Nicholas Dew, and William Gates, "Crossing the Technology Adoption Chasm: Implications for DoD" (Monterey, CA: Naval Postgraduate School, 2008), 22, http://www.acquisitionresearch.net/_files /FY2008/NPS-AM-08-116.pdf.

[124] Christensen, *The Innovator's Dilemma*, 107–8.

[125] Fenn and Raskino, *Mastering the Hype Cycle*, 80.

[126] Ibid., 37.

[127] Ibid., 82.

[128] Ibid., 85.

[129] Ibid; Coughlan, "Crossing the Technology Adoption Chasm," 23.

centered on its long-term market viability and its continued return on investment. This new environment encourages not only the "skeptical" late majority, but also the more cautious laggards, to begin integrating the technology.[130]

D. FACILITATING DIFFUSION AND ADOPTION

In a closed system, perhaps an ideal world, the process of a disruptive technology's diffusion and adoption would always follow a predefined path. For better or worse, however, these processes—diffusion and adoption—occur in the real world, where the lifecycle of a technology constantly interacts with the unpredictability of human nature and market influences. In some cases this interaction can produce unbelievable advances in an individual's quality of life, while in others it can introduce unexpected and uncontrollable risks. Therefore, because "it is often impossible to predict what products and risks will need to be governed even a short time into the future," it is unadvisable for the diffusion and adoption process to proceed completely unabated.[131]

At its core, the hype cycle strives to depict visually how today's "hyperconnected society" handles the constant introduction of the "never-ending waves of potential innovations."[132] One method of guiding the nation's "experimental culture" through this sea of new, and in some cases unrefined, technologies is through the use of change agents.[133] A change agent is an individual or group that works to "influence clients' innovation-decisions" by providing a "communication link between a resource system with some kind of expertise and client system," explains Rogers.[134] Change agents are capable of making a difference in a technology's diffusion and adoption because information about a new technology will spread faster than its adoption.[135] The ultimate goal of these agents is to help avoid the disequilibrium that occurs when a system or

---

[130] Rogers, *Diffusion of Innovations*, 284.

[131] Marchant, Abbott, and Allenby, *Innovative Governance Models,* 58.

[132] Fenn and Raskino, *Mastering the Hype Cycle*, 22–3.

[133] Ibid.

[134] Rogers, *Diffusion of Innovations*, 366 and 368.

[135] Ibid., 214.

structure cannot handle the rate at which changes are occurring within it.[136] Through understanding the requirements and expectations of each adoption group, and thereby working to alter the diffusion and adopting process as needed, change agents can help a technology pass successfully through its strategic inflection points.[137] These added benefits of change agents are especially important when the emerging technology is a disruptive innovation. An alternative to using change agents to facilitate adoption and diffusion is through a "technological ombudsman."

Morison and Toffler were both advocates for instituting regulatory controls in order to protect the general public from unrestricted technological advances.[138] One of their solutions was to introduce what Toffler called a technological ombudsman.[139] Defined by Toffler as "a public agency charged with receiving, investigating, and acting on complaints having to do with the irresponsible application of technology," the technological ombudsman concept was never put into place.[140] Nevertheless, the importance of incorporating the involvement of an ombudsman into the diffusion and adoption process cannot be disregarded. By empowering change agents or ombudsmen to integrate lessons learned from innovators and early adopters into their communication linking endeavors, it is possible for a regulatory or security minded organization to achieve the same goal without any additional bureaucracy. Effectively, this conceptual design would use the innovator and early adopter groups as a risk and threat assessment filter before a disruptive technology continues to diffuse. This approach ultimately provides organizations a method of reducing risks associated with wasting "time, money, and opportunity" when attempting to incorporate regulatory or security controls.[141]

---

[136] Rogers, *Diffusion of Innovations*, 471.

[137] Ibid., 366 and 436.

[138] Morison, *Men, Machines, and Modern Times*; Toffler, *Future Shock*, 428–29 and 431–41.

[139] Rogers suggested a similar concept, which he called an "innovation gatekeeper," but for purposes of clarity this thesis will only use the "technological ombudsman" term; Rogers, *Diffusion of Innovations*, 156; Morison, *Men, Machines, and Modern Times*, 222–24; Toffler, *Future Shock*, 438 and 442.

[140] Toffler, *Future Shock*, 442.

[141] Fenn and Raskino, *Mastering the Hype Cycle*, 21.

E. TIMING REGULATORY CONTROLS WITH THE WINDOW

Once the importance of the window of opportunity—and how it can affect changes in the diffusion and adoption process—is understood, the next step is figuring out how to properly time the introduction of safety and security measures. Due to the dynamic and fluid nature of the innovation process, new technologies need time to diffuse before their impact can truly be understood.[142] Both the technology adoption and hype cycle demonstrate that "the early stages of an emerging technology's development present a unique opportunity to shape its future. But it is an opportunity that does not remain open forever."[143] It is not matter of predicting the future impact of a technology because, as Tenner emphasizes, the involvement of "human culture and behavior" make that an unrealistic goal.[144] Instead, the emphasis must be on using technology forecasting to help identify how a technology is most likely going to develop.

For the purposes of this thesis, technology forecasting is defined as estimates about the future progression of a new technology based "upon an explicit, stated set of relationships, data, and assumptions" that can be reproduced by following a basic "system of logic."[145] By developing and testing each of these projections independently, it is possible to assign each one a different level of confidence. The goal of this process is to help decision makers understand how a new technology may develop over time. However, it is important to note that technology forecasting is only about the technology, it does not take into account the impact that human and market influences can have on a technology as it matures.[146] Historically, industry and technology experts have been the primary source of technology forecasting data.[147]

---

[142] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 44; Kelly and Kranzberg, *Technological Innovation*, ix.

[143] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 62.

[144] Tenner, *Why Things Bite Back*, 271–2.

[145] James R. Bright, "Technology Forecasting Literature: Emergence and Impact on Technological Innovation," in *Technological Innovation: A Critical Review of Current Knowledge*, eds. Patrick Kelly and Melvin Kranzberg (San Francisco: San Francisco Press, 1978), 302.

[146] Bright, "Technology Forecasting Literature," 302–16.

[147] Kelly and Kranzberg, *Technological Innovation*, xvii.

While technology forecasting is not a new concept, the manner in which it is conducted has changed over the years. One of the problems with using only a select group to create a forecast is that their assumptions and decisions can be clouded, or even manipulated, by external influences.[148] For the last few decades, references to a new technology in the media have been one method of measuring its future expectations.[149] In other words, according to Fenn and Raskino, "the more newsworthy an innovation is, the more expectations rise, and that becomes a reinforcing cycle."[150] However, this method shares the same disadvantage as the use of technology experts—when a select group controls assessments, their actions can easily become tainted by alternative agendas. With the advent, diffusion, and adoption of online social media, it is now possible to use information gathered through these networks to conduct social network analysis in near-real time.

Experimentations conducted that gathered information (tweets) from the social media and micro-blogging service Twitter, demonstrate the utility of using social media to help time the window of opportunity. In 2010, Sitaram Asur and Bernardo Huberman of HP's Social Computing Lab were able to use tweets to accurately predict movie box-office revenue.[151] In their paper, they emphasize that social media is "a form of collective wisdom…usually more accurate than other techniques for extracting diffuse information."[152] Concluding that the information gathered through social media is an "effective indicator of real-world performance," Rumi Chunara, Jason Andrews, and John Brownstein of Harvard Medical School tested this theory against the spread of

[148] Kelly and Kranzberg, *Technological Innovation*, xvii; Bright, "Technology Forecasting Literature," 302–16.

[149] Fenn and Raskino, *Mastering the Hype Cycle*, 14.

[150] Ibid.

[151] Sitaram Asur and Bernardo Huberman, "Predicting the Future with Social Media," HP Labs—Advanced Research at HP, Hewlett Packard Development Company, accessed June 13, 2014, http://www.hpl.hp.com/research/scl/papers/socialmedia/socialmedia.pdf.

[152] Ibid.

cholera during the 2010 Haitian outbreak.[153] They showed how tweets could accurately track the spread of the disease up to two weeks faster than official reporting methods.[154] In a similar fashion, "if people are inclined toward adopting an innovation, they will seek out examples that show why it's a good idea."[155] Thanks to society's ubiquitous use of online social media networks, which now contributes to a large part of what generates the hype around a new technology, their actions can be tracked and analyzed.

This type of analysis of big data has given way to the development of a new field of study: social physics. Using big data to explain human behavior, social physics is able to produce timely and accurate results, and provide a cost effective method of timing the window of opportunity.[156]

While technology forecasting helps identify the possible future of a disruptive technology, technology roadmapping is a way for society to try and prepare for the effects it may have after its widespread diffusion.[157] The flexible roadmapping process "provides a structured (and often graphical) means for exploring and communicating the relationships between evolving and developing markets, products and technologies over time."[158] Even though the end product is often thought of as quite simple, the process of creating a roadmap is highly involved and challenging. Thus, the majority of the benefits gained from building a roadmap are derived from its creation process.[159] By bringing together diverse types of people that come from different backgrounds, creating a technology roadmap becomes "an opportunity for sharing information and perspectives

---

153 Brynjolfsson and McAfee, *The Second Machine Age*, 68; Rumi Chunara, Jason Andrews, and John Brownstein, "Social and News Media Enable Estimation of Epidemiological Patterns Early in the 2010 Haitian Cholera Outbreak," *The American Society of Tropical Medicine and Hygiene* 86, no. 1 (2012): 39–44, doi: 10.4269/ajtmh.2012.11-0597.

154 Chunara, Andrews, and Brownstein, "Social and News Media," 39–44.

155 Fenn and Raskino, *Mastering the Hype Cycle*, 34.

156 "Social Physics: A New way of Understanding Human Behavior Based on Analysis of Big Data," MIT Media Lab, accessed August 5, 2014, http://socialphysics.media.mit.edu.

157 Robert Phaal, Clare Farrukh, and David Probert, "Technology Roadmapping—A Planning Framework for Evolution and Revolution," *Technological Forecasting & Social Change* 71, (2004): 22. doi: 10.1016/S0040-1625(03)00072-6.

158 Ibid., 5.

159 Ibid., 23.

and providing a vehicle for holistic consideration of problems, opportunities and new ideas."[160] Ultimately, the roadmap serves as guideline for society to comprehend and adapt to the future implications of an EDT.

Once a technology forecast and roadmap have been considered by a regulatory or security minded organization, the next step in understanding and planning for the future impact of a new technology is developing technological foresight. Ellul explains that foresight is a means of making a realistic assessment of a situation and putting together a plan to mitigate the associated risks of technology adoption. This assessment can be accomplished by taking an almost purely pessimistic view of a disruptive technology whereby society only considers the worst-case scenarios that could stem from the adoption and diffusion of a new technology. Once solutions are developed to these problems, the next step is designing an implementation plan. In his book, *The Technological Bluff,* Ellul demonstrates how technological foresight could help address how society could put together a plan to deal with nuclear power plants when they reach the end of their expected life.[161]

These plans and procedures are an attempt to take advantage of a specific window of opportunity in the adoption and diffusion process of an EDT. An important benefit of this point in time is that only a limited number of adopters—those with the most technological knowledge and highest risk acceptance levels—have been exposed to the new technology. By developing and integrating a continual feedback process by which these early adopters can provide safety and security recommendations, it is possible to mitigate the risks that approximately 80 percent of the total adopting population could potentially face.

When considering an innovation's full lifecycle the timeframe that it is in the chasm and the trough of disillusionment is relatively short. Through using information harnessed from social media networks, in particular the creation or recent passing of a strategic inflection point, it is possible to identify when a window is occurring. Then,

---

[160] Ibid.

[161] Ellul, *The Technological Bluff*, 98–9.

after implementing a method to collect information about future risks from early adopter categories and figuring out how to recognize when the window of opportunity occurs, the next step is putting a plan into place that will protect the population from the potential illicit appropriation of a disruptive technology

F. CONCLUSION

Even though the nation's economy has been built on technological advancement, political institutions are still not capable of addressing concerns of emerging technology in a timely and comprehensive manner, the pace of diffusion and adoption continues to increase bringing about more instances of future shock, and corporations are rarely held accountable when their technology is used with illicit intent. Segal asserts that American society seems to operate under "the painfully naïve assumption that the technological optimism that has historically characterized American society and culture will or must continue unabated."[162] However, as this chapter demonstrates, it is possible to institute a threat mitigation process that will not only allow an emerging technology to follow a traditional path toward ubiquity, but one that could also increase its rate of diffusion and adoption.[163]

The window of opportunity described herein does not represent an all-or-nothing period of action; rather it is the ideal timeframe to introduce new regulatory controls and/or security measures that will not inhibit the technology's future progress based on the state of the technology's infrastructure and the psychology of its user base. By targeting the lull that an emerging technology experiences while in the trough of disillusionment, otherwise known as the chasm that exists between the early adopter and early majority groups, it is possible to inject regulatory controls with the least impact on the technology's further development, diffusion, and adoption.

While it is still possible to enact protective measures after this window, the delay will result in larger implementation hurtles and could ultimately stifle the innovation's further progression. Online social networking sites provide an opportunity to analyze

[162] Segal, *Future Imperfect*, xii.

[163] Kelly and Kranzberg, *Technological Innovation*, iii.

these networks in near real time, thus providing a practical and cost effective method of not only tracking a technology through its adoption cycle and timing the window of opportunity, but also the point at which a new technology reaches critical mass. Additionally, even though rapid prototyping and direct to user distribution has increased the pace of diffusion and adoption, it also provides a "build-in" method of incorporating new threat mitigation controls into consecutive versions of a product's design.

THIS PAGE INTENTIONALLY LEFT BLANK

V. HOMELAND SECURITY

> A prerequisite for effective governance is the ability to assess the safety and security risks of a technology.[164]

Emerging disruptive technologies are completely neutral objects. In their most simplistic form, these new technologies are tools that a society can use in either a positive or negative manner.[165] Despite the steps an inventor may take to mitigate a technology's potential for illicit use, he is ultimately limited by his perspective and imagination. The inventor may become "boresighted" on the problem the technology is being developed to solve, rather than the implications of the technology's impact. In other words, the inventor focuses on what the technology will do, rather than what the technology will change. The problem this creates is that society is left unprotected against the adverse costs associated with adopting a new technology. These unintended and unforeseen adoption consequences that only emerge after the technology has diffused are known as "revenge effects."[166]

While all innovations will incur some level of revenge effects, the reason that EDTs are a more significant concern is because "disruptive technologies often enable something to be done that previously had been deemed impossible. Because of this, when they initially emerge, neither manufacturers nor customers know how or why their products will be used."[167] These concerns are precisely why Edward Tenner's book, *Why Things Bite Back*, argues for the American public to take a cautious approach to allowing new technologies to become part of their daily lives.[168] By understanding the implications associated with an EDT before its widespread diffusion, it may be possible

---

[164] Tucker, *Innovation, Dual Use, and Security*, 19.

[165] Gámez and Nieto-Goméz, "The Case of 'Illicit Appropriation,'" 211.

[166] In order to understand and mitigate the threats that revenge effects pose, it is important to distinguish that the causal factor is not technology itself; rather it is byproduct of the adoption and diffusion process. In other words, "revenge effects happen because new structures, devices, and organisms react with real people in real situations in ways we could not foresee," asserts Tenner; Tenner, *Why Things Bite Back*, 6–9; Rogers, *Diffusion of Innovations*, 470.

[167] Christensen, *The Innovator's Dilemma*, 131.

[168] Tenner, *Why Things Bite Back*, ix–xi and 6–9.

to mitigate future revenge effects. Therefore, as emphasized by Toffler, "we can no longer afford to let…secondary social and cultural effects just 'happen.' We must attempt to anticipate them in advance, estimating, to the degree possible, their nature, strength and timing."[169]

The intention of this chapter is to showcase how domestic law enforcement (in its current design) is willfully unprepared to address the threats that society faces from not only revenge effects, but also the illicit appropriation of an EDT. In order for law enforcement to fill this capability gap, they must embrace a developing intelligence field—homeland security intelligence (HSINT). Ultimately, a properly structured and utilized HSINT community could utilize the criteria outlined in this thesis to provide domestic law enforcement organizations the "edge" they need to combat future technology related threats.

A. HOMELAND SECURITY INTELLIGENCE

"Government bureaucracies designed to maintain a stable, fair, and open society are increasingly being outpaced by changing technologies and emerging trends," asserts Christopher Kluckuhn.[170] If the rate of public adoption of an EDT exceeds the ability of the government or private sector to institute security measures, then the public may face unforeseen and unintentional threats to its safety. Furthermore, if a new technology is appropriated from the task for which it was designed and used criminally, the security implications become even more complex and urgent. Rather than attempt to regulate or police all EDTs, the United States must endorse the further development and integration of HSINT.

169 Toffler, *Future Shock*, 438.

170 Christopher Kluckhuhn, "An Examination of Four Successes in the Coast Guard's Innovation Program and Implications for Innovation within Homeland Security" (master's thesis, Naval Postgraduate School, 2008), 1, http://hdl.handle.net/10945/4216.

In the wake of 9/11, DHS was created. Its overall mission is to "ensure a homeland that is safe, secure, and resilient against terrorism and other hazards."[171] The broad and all-encompassing nature of this mission could be compounded exponentially by the illicit appropriation of an EDT. As Brynjolfsson and McAfee assert, as technologies become more advanced and ubiquitous the people who adopt them may not be "both sane and well intentioned."[172] Even more concerning is that "the physical limits on how much damage any individual or small group could do are becoming less and less constrained."[173] Therefore, because it is unrealistic for DHS to try and protect against all possible threats, it must find a way to screen and assess the threats it will attempt to mitigate with its limited resources.

Raw information is of little use to decision makers within the DHS simply because of the vast amount that is collected on a daily basis by numerous domestic law enforcement agencies. In many cases, raw information can be more of a distraction than a force multiplier. As emphasized by Ian Lustick in *Trapped in the War on Terror*, the FBI's reaction to 9/11 was to investigate every single tip it received that had anything to do with terrorism. Despite the fact that within the first week after 9/11 the FBI received more than 96,000 leads (by the end of the first year, it was more than 400,000), it was determined to investigate every one—no matter how insignificant or irrational the tips may have appeared. Lustick contends that the FBI needed to institute a form of "triage" that would allow it to focus on the more credible and timely threats. Effectively, what Lustick is stating is that the FBI needed intelligence personnel to analyze the tips before field agents started their investigations.[174]

---

171 "Our Mission," U.S. Department of Homeland Security, accessed May 20, 2014, http://www.dhs.gov/our-mission; Specifically, DHS defines its five homeland security core mission areas as, "prevent terrorism and enhancing security, secure and manage our boarders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters."

172 Brynjolfsson and McAfee, *The Second Machine Age*, 253.

173 Ibid.

174 Lustick appropriates the term triage from the medial field's method of classifying patients during a mass causality event. Because of staffing and supply limitations every patient cannot be treated the same, therefore, this process ensures that the patients that are more critically injured will get treated first. Ian Lustick, *Trapped in the War on Terror* (Philadelphia: University of Pennsylvania Press, 2006) 1–3.

As outlined in the Department of Defense *Joint Intelligence Publication* (JP-2), "[i]nformation is of greatest value when it contributes to or shapes the commander's decision-making process by providing reasoned insight into future conditions or situations."[175] While it is possible to collect massive amounts of data easily these days, the information is relatively worthless until qualified intelligence personnel analyze it. This process of analysis is what turns raw data into usable intelligence. Thus, contributing to what Mark Lowenthal considers in the journal *Intelligence and National Security* the single most important purpose of intelligence—helping to "reduce uncertainty."[176] Since the implications of EDTs diffusion and adoption are an area of technological development that introduces a high level of uncertainty, it is necessary for domestic law enforcement to develop a process that will help mitigate any of newly created safety and security threats.

In order to use intelligence to help mitigate an EDT threat, it is critical for the domestic intelligence community (IC) to rethink the first two elements of intelligence: collection and analysis.[177] Historically, the determining factor of an analyst's qualifications is based on the medium of the collected information (e.g., someone who analyzes signal intelligence [SIGINT] is a SIGINT analyst). In other words, the type of information is what defines the analyst.

However, unlike other intelligence disciplines that are defined by the specific manner in which analysts collect and focus their efforts primarily on foreign collection, domestic intelligence is an amalgamation of all the other "INTs" and specifically directed at a democratic populace.[178] Unofficially referred to as HSINT, the basis of this discipline requires intelligence personnel to navigate a diverse set of collection methods

---

[175] Director for Intelligence (J-2), *Joint Intelligence.* JP 2-0 (Washington, DC: U.S. Government Printing Office, 2013), accessed February 12, 2014, xi. http://www.dtic.mil/doctrine/new_pubs /jp2_0.pdf.

[176] Mark Lowenthal, "Towards a Reasonable Standard for Analysis," *Intelligence and National Security* 23, no. 3 (2008): 313, doi: 10.1080/02684520802121190.

[177] Lowenthal goes on to state that the other two elements of intelligence are counter-intelligence and covert action. Mark Lowenthal, *Intelligence: From Secrets to Policy*, 5th ed. (Los Angeles: Sage Publications, 2012), 14.

[178] All other "INTs" used here is referring to SIGINT, human intelligence (HUMINT), measurement and signature intelligence (MASINT), etc.

within a complex operating environment in order to support its customer, domestic law enforcement agencies. Therefore, HSINT challenges the traditional IC's norms, and requires the analyst to define the type of information that is needed based on the current case—a HSINT analyst may need imagery intelligence (IMINT) for the first case, and communication intelligence (COMINT) for second. Additionally, in the case of EDTs, HSINT can also act as a method to screen raw information prior to its distribution either to domestic law enforcement agencies or the American public.

Domestic law enforcement needs creditable intelligence on "the subset of emerging technologies that are potential game changers because they could result in harmful consequences far more serious than is possible with existing technologies."[179] Because it *is not* possible to accurately predict how or at what rate a new technology will diffuse through a society, how a society will adapt to the technology, or how a technology will develop once it is adopted, it *is* possible for properly trained HSINT personnel to focus specifically on how to mitigate the illicit appropriation of the new capability that an EDT will introduce.

For example, the diffusion of 3D printers permits individuals to create and manufacture three-dimensional objects at home. While the intended usage is for safe and innocent at-home projects, the technology combined with online collaboration enables users to make high quality firearm parts and high-capacity magazines by simply downloading a CAD file.[180] This manner of production not only circumvents the requirement of a Type 07 federal firearms license, but it also provides a method for those with felony convictions to easily acquire a firearm.[181] In this case, HSINT personnel could evaluate whether or not the diffusion of a *high quality*, *precision*, *unregulated*, *and*

---

[179] Tucker, *Innovation, Dual Use, and Security*, 3.

[180] These files contain all of the information needed so that a 3D printer can create an object. While conventionally they require significant experience and education to create, they are now available for download via online collaboration sites. This method of acquiring a CAD file removes the necessity of individuals having any background knowledge in gunsmithing or engineering in order to build a working firearm. Also, as an aside, in this situation the internet, an EDT in itself, is acting as a backbone technology potentially multiply the threat from 3D printers.

[181] "Listing of Federal Firearms Licensees (FFLs)—2014," Bureau of Alcohol, Tobacco, Firearms and Explosives, United States Department of Justice, accessed May 21, 2014, https://www.atf.gov/content /firearms/firearms-industry/listing-FFLs.

privacy protected at-home manufacturing device could be illicitly appropriated, and then assess if there is a way to mitigate this threat prior to its further adoption.

By focusing on the new capability that an EDT introduces, the HSINT discipline can be distinguished from other new prevention methods that utilize big data and other similar technologies in an attempt predict future crimes. The problem with this "predictive policing" is that it simply indicates the *probability* of an offense occurring based on historical data, and does not take into account the human element. Additionally, "predictive indicators are not universal. [So,] security specialists may have to proceed on a case-by-case basis when seeking to anticipate and foil deadly innovations," concludes Rasmussen and Hafez.[182] Due to HSINT's use of information from all of the traditional intelligence collection methods (the other "INTs"), this brand of intelligence can be adapted to address the varying types of cases that domestic law enforcement agencies face on a daily basis. As a testament to the DHS's mission of all hazard protection, it created a specialized division of its Science and Technology (S&T) Directorate that specifically focuses on emerging technological based threats—aptly named the Emerging Threats Branch.

In light of the vast list of DHS responsibilities, it is unrealistic to insist that the task of mitigating threats from EDTs should become a primary mission. However, because the nature of the threat is far-reaching (i.e., it is not limited to a defined vulnerability within a specific industry), it cannot simply be ignored and restricted to a predominantly reactive protection strategy.[183]

---

[182] Rasmussen and Hafez, "Terrorist Innovations in Weapons of Mass Effect."

[183] For this very reason, the Emerging Threats Branch is tasked with "identifying over-the-horizon technologies by ascertaining potential future threats." Its proactive approach to the EDT threat supports the domestic IC's efforts to assess potential responses to an emerging threat, integrate with other divisions within the S&T IC, and identify current capability gaps. However, to accomplish these goals the Emerging Threats Branch would require a staff with an in-depth understanding of how to leverage multiple intelligence methods to provide usable information for decision makers as they try to navigate the complexities of managing risk within the innovation process. There is minimal information available at the unclassified level about the Emerging Threats Division because it is part of the Department's Special Program Division. "Science and Technology Special Programs Division," Homeland Security, U.S. Department of Homeland Security, accessed May 21, 2014, http://www.dhs.gov/st-special-programs-division.

B. CONCERNS AND SOLUTIONS

Even though it is possible to define what HSINT is and identify a need for its existence, there is no guarantee that this intelligence discipline will ever be fully endorsed and accepted by the American public. Hank Crumpton sums up the concerns over widespread domestic intelligence collection by stating that, "excessive defense brings unintended negative consequences that may far outweigh the expected benefits."[184] In this case, the American public's concerns over domestic intelligence are not limited to the actions of the DHS and accepting HSINT as an intelligence discipline; rather the issues are much larger and directed at the domestic IC as a whole.

Specifically, two of the hurdles that domestic IC must overcome before it can be widely accepted into a democratic populace are civil liberty issues and obscure oversight structure. In the United States, citizens' civil liberties are detailed in the Constitution, specifically the Bill of Rights. Recently, concerns over domestic intelligence collection methods pose the question as to whether or not there is a tradeoff between the need for increased security and being able to protect an individual's civil liberties. Ideally, as stipulated in the 9/11 Commission report, there is no reason for this type of tradeoff to occur; but, in reality, on more than one occasion the U.S. government has violated an individual's civil liberties under the guise of national security.[185] Examples of such civil liberty infringements include the internment of Japanese Americans during World War II, and more recently, the profiling of Muslim Americans after 9/11.

In many ways, these governmental actions are strikingly similar to how the National Security Agency (NSA) accidently collects information on American citizens. Even though the information (referred to within the community as inadvertent collection) is not releasable to domestic law enforcement agencies and it is quickly disregarded, an individual's civil liberties were still violated. If HSINT or any type of domestic

---

[184] Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 203.

[185] Report of the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, official government edition (Washington, DC: U.S. Government Printing Office, 2004).

intelligence collection becomes an accepted intelligence discipline, then more likely than not the chances of inadvertent collection—and, hence, civil-liberties violations—will increase.

At the same time, individuals who wish to cause harm often exploit, whether intentionally or unintentionally, the Constitution's civil liberty protections in order to hide the preparation of an attack. The predicament that law enforcement faces is that there are those within American society that have a preconceived notion that all domestic intelligence collection is detrimental to the nation's democratic environment. However, with respect to mitigating threats from EDTs, it is possible to restrict HSINT personnel to focusing specifically on the capabilities of a new technology and the manner in which it could be illicitly appropriated. This approach would prevent domestic intelligence collection on specific individuals, thereby greatly reducing the potential for civil liberty violations.

An additional benefit of concentrating domestic collection efforts away from specific individuals is that the intelligence concerning the EDT could be distributed outside of the domestic IC. As an example, the information that the HSINT community collects could be provided to the inventor and manufacturer of the technology so that they could modify future releases, for example, by creating a Version 2 of their product that reduces the technology's risk of illicit appropriation. As illustrated by Crumpton, "superior intelligence and superior strategy, founded on a partnership with greater America, can also achieve victory with minimized cost to civil liberties at home."[186] Even more significantly, if this cooperative approach could go beyond just EDT threats and be adopted for other technologically related threats, then the overall manner in which DHS and other domestic law enforcement agencies protect the public does not necessitate a change. Instead, the public would only need to ensure that domestic intelligence actions have proper oversight to prevent the intelligence agencies from overstepping their specified boundaries.

[186] Sims and Gerber, *Transforming U.S. Intelligence*, 215.

C. CONCLUSION

All technology is not bad. In agreement with Eduardo Calvillo Gámez and Rodrigo Nieto-Gómez, "if the process of committing a crime or illegal conduct is properly regulated, then the technology used to pursue it would not need to be punished."[187] However, some of the concerns raised with respect to domestic law enforcement intelligence collection are based on a perceived tradeoff between security and civil liberties. In other words, if domestic law enforcement were to restrict access to a new technology due to its potential for illicit appropriation, it could very well violate an individual's civil liberties. While perhaps counter-intuitive, in order to mitigate this concern domestic intelligence collection needs to focus its attention on the new capabilities that technology introduces not the technology itself.

In order for the DHS to try and proactively protect the American public from EDT based threats, it must embrace the development of a domestic intelligence discipline—homeland security intelligence. Through proper training and oversight HSINT professionals would be capable of protecting American citizen's civil liberties, while actively assessing the potential threats that may stem from a new technology.[188] However, Tucker emphasizes, "as our complex technological civilization continues to accelerate into an uncertain future, government alone cannot undertake the challenge of managing the risks of emerging…technologies."[189]

---

[187] Gámez and Nieto-Goméz, "The Case of 'Illicit Appropriation,'" 226.

[188] Rodrigo Nieto-Goméz, "Power of 'the Few' A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment," *Homeland Security Affairs* 7, no. 18 (2011): 16, http://hdl.handle.net/10945/24994.

[189] Tucker, *Innovation, Dual Use, and Security*, 337.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. IS REGULATION THE ANSWER?

> No single regulatory agency, or even group of agencies, can regulate…emerging technologies effectively and comprehensively.[190]

Technological innovation is a driving force behind the prosperity of the U.S. economy.[191] "Although the government theoretically plays a minor role in a free-enterprise economy, the U.S. government has become increasingly involved in fostering new technology," insists Patrick Kelly and Melvin Kranzberg.[192] Two of the ways that it directly contributes to the development of technology are funding and regulation, both of which are subject to constant oversight.[193] Because inventing new technologies is a costly endeavor that cannot guarantee any type of return on investment, the majority of the funds the government provides are to businesses within established industries.

This selective funding approach often limits the type of development to creating sustaining technologies. When a sustaining technology is introduced, such as the collision-avoidance systems in the automobile industry, it is done in a controlled and orderly fashion. This process has been refined over the years to ensure that these new systems are tested thoroughly, and proven to be a beneficial safety feature, before their widespread adoption is permitted. One such example is the U.S. Department of Transportation's support to the development and integration of vehicle-to-vehicle (V2V) communications for improving roadway safety.[194] While this technology may revolutionize transportation, government and industry are jointly developing and implementing it in a controlled manner with a specific application. However, EDTs do not have any prescribed protective measures in place to evaluate them, which introduces significant adoption and diffusion related risks to an unsuspecting public.

---

[190] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 136.

[191] Brynjolfsson and McAfee, *The Second Machine Age*, 72–73; Kelly and Kranzberg, *Technological Innovation*, iii.

[192] Ibid., x; Marchant, Abbott, and Allenby, *Innovative Governance Models*, 256.

[193] Kelly and Kranzberg, *Technological Innovation*, x.

[194] "Connected Vehicles," National Highway Traffic Safety Administration, accessed March 11, 2014, http://icsw.nhtsa.gov/safercar/ConnectedVehicles/pages/v2v.html.

Historically, the tendency has been for corporations and society to decide how an emerging technology will be controlled and used through a "trial and error" type of process. There is no formalized process to consider the societal impact of unforeseeable and unexpected threats that could stem from the new technology's integration (its revenge effects). Therefore, only when the threats from the technology become uncontrollable does the government finally get involved. A contemporary example of this is the emergence of online peer-to-peer payment systems like Bitcoin. Bitcoin was left to proliferate without government involvement or recognition until it was adopted as a safe haven for anonymously transferring money for illicit activities and the collapse of Mt. Gox, a bitcoin exchange.[195] The problem with this method of protection is that governmental based actions are typically a tediously slow and complex process.[196] Additionally, by relying on a bureaucratic approach, the government would be restricted to only enacting reactive security and safety measures.

While some Americans associate the term "regulation" with "restriction," there are cases where regulation, for instance, setting industry standards, helps to proliferate new technologies and increase their rate adoption. According to the Porter hypothesis, strict regulatory controls can enhance competitiveness between companies by challenging them to meet new standards; companies that can develop the new technology the fastest will have the advantage of being the first to bring it to market.[197] In the United States, funding and regulation tend to serve as enablers to encourage companies to innovate because the government does not micro-manage every aspect of the R&D process.

The concern, however, is that when large established companies are working with the government to innovate, they tend to protect their market share fiercely by either

---

[195] Mt. Gox was one of the foremost bitcoin exchange networks, and it collapsed when it was hacked and lost the majority of the bitcoins that it held. Unlike holding funds in a bank, bitcoins are an unregulated monetary vehicle and therefore not protected by an organization like the Federal Deposit Insurance Corporation (FDIC).

[196] *U.S. Congress, House, Joint Economic Committee, The Cost of Government Regulation: Hearings before the Subcommittee on Economic Growth and Stabilization*, 95th Cong. (1978).

[197] Even though the Porter hypothesis specifically mentions environmental, health, and safety regulations, I believe that it can be applied more broadly. Michael Porter and Claas van der Linde, "Toward a New Conception of the Environment-Competitiveness Relationship," *The Journal of Economic Perspectives* 9, no. 4 (1995): 97–118, http://www.jstor.org/stable/2138392.

buying up or forcing smaller companies out of the market.[198] Thus, it is frequently difficult for a new company to enter one of the nation's established industry sectors because large corporations control the majority of the market. This monopolistic obstacle can become a form of self-regulation that inhibits the introduction of new disruptive technologies. In this book, *The Master Switch*, Tim Wu illustrates this dynamic with a historical example. In 1934, Wu writes, AT&T's Bell Labs developed an answering machine but kept it from the public because the company did not feel the technology was commercially viable. At the time, AT&T executives were concerned that the recording of phone calls would adversely affect their customers' telephone usage. AT&T's actions limited the development of magnetic tape technology (the medium used for recording messages) for the next 15 years.[199]

Through the introduction of disruptive technologies, smaller companies can challenge the market share of larger corporations. As evidenced by the shift from CDs, telephones, and postal mail to MP3s, cell phones, and email, disruptive technologies enable new companies to absorb the market share from larger established corporations, and in some cases, create completely new and independent markets.

One could argue that this type of competition is a manifestation of Adam Smith's invisible hand theory; requiring these companies to develop disruptive technologies the market is working to regulate itself. Because they are often working in unchartered territory, companies operating outside of an established industry tend to take a more laissez-faire approach to doing business; therefore they have no defined filter for a technology to pass through before it is released to the public. Barring any change in industry's passivism toward new disruptive technologies, the first indication of a new threat from the illicit appropriation of a technology may be in the form of an attack on American soil. This type of threat, one that is widespread and contains a multitude of

---

[198] Thomas K. McCraw, "American Capitalism," in *Creating Modern Capitalism: How Entrepreneurs, Companies, and Countries Triumphed in Three Industrial Revolutions*, ed. Thomas K. McCraw (Cambridge: Harvard University Press, 1998), 327.

[199] It was not until another inventor started researching magnetic tape that the technology began to progress. This stagnation was because Bell Labs' research into the technology was purposely hidden until 1990, when a historian accidently stumbled across it. Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Alfred A. Knopf, 2010), 106.

unknown factors, is precisely why the government has previously explored different methods of understanding new technologies when they are still in their infancy.

A. UNSUCCESSFUL ATTEMPTS

Whether intentional or not, there is a symbiotic relationship between the U.S. government and the development of new technologies.[200] For example, the government "contributes over one-half the nation's R & D funds."[201] In an attempt to understand new technologies and make the right choice with taxpayer's money, the government has formed such groups as the Office of Technology Assessment (OTA), and more recently, the Emerging Technologies Interagency Policy Coordination Committee (ETIPC). While full of good intentions and ideas, both of these groups have failed in one form or another to provide today's decision makers with timely and actionable information.

The OTA was established by Congress through the Technology Assessment Act of 1972 "as an aid in the identification and consideration of existing and probable impacts of technological applications," whether beneficial or adverse.[202] Proposed by Congressman Emilio Q. Daddario, the driving force behind the OTA's creation was the skepticism surrounding the adoption of new technologies that began to proliferate in the mid to late 1960s. Congress stated in the act, "it is essential that, to the fullest extent possible, the consequences of technological applications be anticipated, understood, and considered in determination of public policy on existing and emerging national problems."[203] Working toward that goal, the OTA produced more than 750 studies, totaling more than 100,000 pages, on such topics as "Access to Space: The Future of U.S.

[200] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 44.

[201] Kelly and Kranzberg, *Technological Innovation*, x.

[202] "Office of Technology Assessment Act," The Technology Assessment Act, The Trustees of Princeton University, accessed June 23, 2014, http://www.princeton.edu/~ota/ns20/act_f.html.

[203] Ibid.

Space Transportation" (April 1990) and "World Population and Fertility Planning Technologies: The Next 20 Years" (February 1982).[204]

Due to budgetary constraints and criticisms over its effectiveness its shutdown in 1995 left Congress without a method for the government to get nonpartisan and objective advice and analysis on the potential impact of EDTs, there has been a movement in recent years to reopen the office. Perhaps due to the fact that many of the office's findings are still relevant today, Hillary Clinton and others within the current administration have advocated for the OTA's reinstatement.

More recently, in 2010, the Obama Administration formed the ETIPC. Made up of the Office of Science and Technology Policy, the Office of Information and Regulatory Affairs, the Office of the United States Trade Representative, and assistant-secretary level members from 20 other federal agencies, it is tasked with accessing, "the policy implications of emerging technologies, including the need for 'risk-benefit-based oversight mechanisms that can ensure safety without stifling innovation, stigmatizing emerging technologies, or creating trade barriers.'"[205] However, as Tucker points out, despite this mandate the committee does not have legal authority, requisite experience, or even a security mandate to mitigate newly developed threats.[206] Instead, it is primarily concerned with assisting the development of emerging technologies in the infotech, biotech, and nanotech industries.[207]

B. FLEXIBILITY VERSUS RIGIDITY

In the United States, privately funded firms that conduct research and development outside of traditional industry norms can do so without any formal oversight. While this freedom has enabled the development and diffusion of disruptive

---

[204] Ibid.

[205] Heather Evans, "Emerging Technologies IPC Has Inaugural Meeting," Office of Science and Technology Policy, The White House, last modified May 15, 2010, http://www.whitehouse.gov/blog/2010/05/15/emerging-technologies-ipc-has-inaugural-meeting; Tucker, *Innovation, Dual Use, and Security*, 330–1.

[206] Ibid.

[207] Evans, "Emerging Technologies IPC Has Inaugural Meeting;" Tucker, *Innovation, Dual Use, and Security*, 330–1.

technologies, it has also created an "extreme form of competitive individualism."[208] The primary motivation to push a new technology toward ubiquity is competition and profit, seemingly ignoring the social costs.[209] Even though the introduction of state-of-the-art technology enables businesses to stay ahead of their competition; these new innovations may also come with unknown safety and security concerns.

To ensure the safety and security of its population the European Union has chosen to adopt a regulatory measured called the "precautionary principle."[210] This principle grants policy makers, when there is a "danger associated with a procedure or product placed on the market," the power to require the producers of a technology to "prove the absence of danger" associated with their product.[211] While there is a movement within the U.S. to introduce a similar type of regulatory control, advocates against its implementation argue that a "better safe than sorry" approach to technological innovation does not align with American ideals.[212] By its nature, any type of innovation exploration is going to be inherently risky, and allowing policy makers the power to directly stifle technological progress based on "salutary political or moral motivations" would only intensify the nation's rigid regulatory environment. Due to the government's liner framework (i.e., the current process of creation, distribution, and then enforcement of rules and regulations), it is unable to efficiently and expeditiously adjust rules and regulations to reflect market or social changes.[213]

A contemporary example of how lack of regulatory flexibility can impede the use of new technology is the Federal Aviation Administration's (FAA) ban on commercial

---

[208] McCraw, "American Capitalism," 348.

[209] Ibid.

[210] Communication Department of the European Commission, "The Precautionary Principle," Europa: Summaries of EU legislation, European Union, last modified April 12, 2011. http://europa.eu/legislation_summaries/consumers/consumer_safety/l32042_en.htm.

[211] Ibid.

[212] Cass Sunstein, "The Paralyzing Principle," *Regulation* (2002): 32, http://object.cato.org/sites/cato.org/files/serials/files/regulation/2002/12/v25n4-9.pdf

[213] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 254 and 256; Tucker, *Innovation, Dual Use, and Security*, 328.

drone usage.[214] As the cost and complexity of commercial drone systems decreased, the proliferation of the technology increased. Thus, the door opened for widespread drone usage in a multitude of different industries such as journalism, real estate, videography, etc., none of which have experience with the rules and regulations associated with operating an air vehicle within U.S. airspace. Even though the widespread public and private interest in commercial drone usage began around 2010, the FAA failed to prepare a set of rules and regulations that specifically address the operation of drones within U.S. airspace.[215] Because of this lack of foresight and driven by security concerns, the FAA chose to issue a blanket policy banning the use of drones (except for those granted an exemption, which is decided on a case-by-case basis) until it formulated a set of rules and regulations that governed their use. Congress has called for them to complete this by September 2015. The inability of the FAA to expedite necessary regulatory controls over commercial drone usage could inhibit or stall the further development and usage of this new technology—which is an example of the "hidden cost" of government regulation.[216]

The complexities involved with introducing oversight measures into the development, diffusion, and adoption of EDTs, are very similar to those faced in the biotechnology field. Advances in biotechnology are plagued with dual-use concerns, and the efforts to prevent the illicit use and potential appropriation of new breakthroughs risk inadvertently inhibiting the innovation's development, diffusion, and adoption. In order to address this concern the biotechnology field has begun to shift toward a flexible governance model because its innovations, "are advancing so fast that more rigid measures would rapidly become obsolete."[217] As described by Lori Knowles, the three types of oversight used in biotechnology are "hard law (treaties, statutes, and regulations), soft law (voluntary standards and guidelines), and informal measures

---

[214] Jonathan Wiener, "The Regulation of Technology, and the Technology of Regulation," *Technology in Society* 26, (2004): 489, doi: 10.1016/j.techsoc.2004.01.033.

[215] In 2010, the low-cost and relatively easy to control Parrot AR.Drone quadcopter was first introduced. In 2011, the University of Nebraska-Lincoln's College of Journalism and Mass Communications opened the nation's first Drone Journalism Lab.

[216] U.S. Congress, The Cost of Government Regulation.

[217] Tucker, *Innovation, Dual Use, and Security*, 45.

(awareness raising, professional codes of conduct)."[218] When used together these mechanisms can form a blanket of protection against illicit use and appropriation by ensuring responsible usage. Even though the government cannot institute an all-encompassing approach to protect the public against the illicit use and appropriation of all EDTs, it can assist in the establishment of an oversight framework that allows for rapid and frequent changes.[219] It is now possible "for governance systems to develop simultaneously with technologies, permitting proactive rather than reactive management structures."[220]

Two types of flexible regulation methods form alternatives to the typical command-and-control design (traditional or direct regulation where the government regulates industry): "adhocracies" and "ambidextrous organizations." The benefit of an adhocracy is that it provides a dynamic operating environment that is free from bureaucracy.[221] A well-known successful example is the DARPA. Ambidextrous organizations are those that are designed to focus on both short- and long-term goals simultaneously.[222] Eastman Kodak is a good example of a company that would have benefited from a more ambidextrous design because its structure was, "so captivated by its past that it was too slow in changing along with its environment," which ultimately lead to its downfall.[223]

Richard Stewart lists four different ways that regulation could stifle innovation in his paper on "Regulation, Innovation, and Administrative Law." They are, "(1) by imposing technical constraints on firms; (2) by forcing firms to make additional

---

[218] Tucker, *Innovation, Dual Use, and Security*, 45.

[219] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 256.

[220] Tucker, *Innovation, Dual Use, and Security*, 45; Marchant. Abbott, and Allenby, *Innovative Governance Models*, 62.

[221] Robert Waterman, *Adhocracy: The Power to Change* (New York: W.W. Norton, 1992).

[222] Tushman, *Winning Through Innovation*; Robert Duncan, "The Ambidextrous Organization: Designing Dual Structures for Innovation," in *The Management of Organization Design, Vol. 1. Strategies and Implementation*, ed. Ralph Kilmann, Louis Pondy, and Dennis Slevin (New York: North Holland, 1976), 167–188.

[223] Josh Kerbel, "The U.S. Intelligence Community's Kodak Moment," The National Interest, May 15, 2014, http://nationalinterest.org/feature/the-us-intelligence-communitys-kodak.

expenditures or outlays; (3) by causing uncertainty; and (4) by causing delay."[224] Similar to the compliance burdens that described by Luke Stewart, these concerns ultimately "divert time and money from innovative activities to compliance efforts" inhibiting the fluid nature of the innovation process.[225] Through embracing flexible regulatory frameworks, along with an in-depth "data gathering and evaluation" process, it is possible for regulation to mature alongside a new technology and break free from the historically rigid U.S. regulatory structure.[226] However, in order for this type of regulatory design to be effective with EDTs, it "must be implemented in a political environment in which various stakeholders and interest groups will have their say."[227]

C. APPROPRIATING A REGULATORY DESIGN

The purpose of pursuing alternative regulatory methodologies is not to remove the government from the process. Rather it is to ensure that the government delegates regulatory authority to those that are informed and capable of making intelligent decisions about EDTs.[228] Through the appropriation of the cooperative regulation design of the securities market, it is possible to construct an effective and efficient regulatory governance for EDTs.[229] Cooperative regulation allows for advisory committees to be supported by a formal governmental agency, whereby the government backs this form of

[224] Richard Stewart, "Regulation, Innovation, and Administrative Law: A Conceptual Framework," *California Law Review* 69, no. 5 (1981): 1279, http://www.jstor.org/stable/3480247.

[225] Stewart, "The Impact of Regulation on Innovation," 2.

[226] Marchant, Abbott, and Allenby, *Innovative Governance Models*, 59.

[227] Tucker, *Innovation, Dual Use, and Security*, 79.

[228] Richard Epstein, "Can Technological Innovation Survive Government Regulation?" *Harvard Journal of Law & Public Policy* 36, no. 1 (2013): 103, http://www.harvard-jlpp.com/wp-content /uploads/2013/01/36_1_087_Epstein_Tech.pdf; Stewart, "The Impact of Regulation on Innovation," 23.

[229] Cooperative regulation is a term coined in 1964 by the former commissioner of the SEC: Manuel Cohen. Manuel Cohen, "Cooperative Regulation," Commission Speeches and Public Statements Archive: 1964, U.S. Securities and Exchange Commission, last modified October 10, 2007, http://www.sec.gov /news/speech/speecharchive/1964speech.shtml.

self-regulation. It differs from co-regulation because the government's involvement (in cooperative regulation) remains mostly passive until advisory committee requires its authority.[230]

Specifically for EDTs, the cooperative regulation would include an emerging technologies advisory committee (eTAC) that would be backed by the DHS S&T Directorate. Additionally, the committee, DHS, and inventors would benefit from the inclusion of independent and objective technological savvy research, perhaps an emerging technologies assessment board (eTAB) modeled after the OTA. Finally, "because of limitations of budget, personnel, time, and working experience, regulators cannot hope to develop in-house all the information and specialized experience needed to make effective regulatory judgments."[231] Therefore, eTAC must allow inventors an opportunity to provide feedback during the evaluation process.[232]

Functionally, eTAC would use its understanding of the hype cycle, technology adoption cycle, and the chasm to develop preliminary reports on the EDTs it considers candidates for illicit appropriation. Copies of these reports would then be provided to the targeted technology's inventor for comment. A finalized version of the preliminary report that incorporates the inventor's feedback would then be sent to eTAB. The board would then conduct in-depth research into the technology and provide the eTAC with a report that details the development and functionality of the technology along with any current safeguards. In order for this regulatory design to function properly, it is imperative that the reports provided by eTAB only contain factual data. eTAC's responsibility would be to conduct a final evaluation based on the eTAB's research, and then allow the inventor another opportunity to provide feedback on the finalized report. Lastly, the report with the inventor's comments would be forwarded to the DHS S&T directorate (perhaps the S&T Special Programs Division-Emerging Threats Branch).

---

[230] Glen Hepburn, "Alternatives to Traditional Regulation," Organization for Economic Co-operation and Development, accessed February 6, 2014, http://www.oecd.org/gov/regulatory-policy/42245468.pdf.

[231] Stewart, "Regulation, Innovation, and Administrative Law," 1354.

[232] Hepburn, "Alternatives to Traditional Regulation;" Stewart, "Regulation, Innovation, and Administrative Law," 1256, 1354–5, and 1359.

The intention of this governmental design—cooperative regulation—is to harness the benefits inherent in "governance by assessment."[233] Regulation that is "made-to-order to satisfy government demands" would be ineffective toward mitigating threats from EDTs.[234] Furthermore, because cooperative regulation is based off a modified self-regulatory model, it should prove to be "less costly than traditional command and control regulation," and better suited "to the rapid changes of technology in the innovation age."[235] By using an existing governmental body in a supporting role, the DHS S&T Directorate, it would ensure that the government's involvement is kept to a minimum and prevent the establishment of an entirely new agency dedicated specifically to mitigating threats from EDTs.

Additionally, instituting only a technical advisory committee (that is, forming a body without a research branch) could cause the group to focus primarily on the technology rather than the new capability it introduces.[236] Instead, this governance model would not only provide an in-depth understanding of a new technology, but also a body of experience to evaluate safety and security concerns alongside the inventor. The involvement of private industry in the evaluative process, along with encouraging them to provide feedback on the preliminary and finalized reports, serves a dual purpose. It not only builds trust between industry and the regulatory process, but it also is a necessary requirement of any method that attempts to mitigate threats from EDTs.[237] As Stewart illustrates, "with the support and cooperation of all interested parties, these institutes could advance relevant technical learning through a nonadversary process, saving resources and time and promoting confidence in the technical basis of regulatory policy."[238]

---

[233] Wiener, "The regulation of technology," 485.

[234] Solveig Singleton, "Regulatory Obstacles to Innovation: Is Self-Regulation the Answer?" CATO Institute, accessed Feb. 2, 2014, http://www.cato.org/pubs/wtpapers/990913catoself.html.

[235] Ibid.

[236] Stewart, "Regulation, Innovation, and Administrative Law," 1359.

[237] Ibid., 1354.

[238] Stewart, "Regulation, Innovation, and Administrative Law," 1359.

Ultimately, for eTAC to be truly effective the committee must be an independent multi-industry backed organization supported by both public and private funding. Similar to the manner in which the FDA is funded, eTAC could benefit from fees paid by inventors to expedite the committee's evaluation process. Another potential source of funding could come from what Toffler calls a "technological insurance pool." Corporations conducting R&D into new technologies would have to pay liability premiums so that "society would not need to wait for a disaster before dealing with its technology-induced problems" (at least the financial related aspect of it).[239] The concept of a liability insurance pool would be a proactive approach to the threats that may stem from EDTs, and it would indirectly encourage corporations to be responsible for testing their new technology before they begin the diffusion process. In agreement with Toffler, "if self-policing works, it is preferable to external, political controls."[240]

D. CONCLUSION

Any EDT risk mitigation decisional framework, in order to not stifle innovation, will need to include flexible levels of control. If the adoption or diffusion of an EDT does not pose a threat, controls should be sidelined until the situation changes. Furthermore, a requirement for adaptive governance must be based on the ideal that technology itself is not the threat; rather it is the new capability that the technology provides.[241]

The involvement and acceptance of public and private industry with any instituted method of EDT threat mitigation is essential, and should be encouraged through the development of a cooperative process. This partnership can be formed through the creation of an eTAC, with authority that stems from the DHS S&T Directorate, and an iterative feedback process for inventors. Finally, the inclusion of an eTAB modeled after the OTA would ensure the committee has the requisite knowledge it needs to make informed recommendations and assessments. The ultimate goal is a push and pull form of education at every level and on both sides of the innovation development, diffusion, and

[239] Toffler, *Future Shock*, 444.

[240] Ibid., 443.

[241] Ibid., 440; Tucker, *Innovation, Dual Use, and Security*, 39 and 82; Marchant, Abbott, and Allenby, *Innovative Governance Models*, 8–9.

adoption processes. Innovators need to be educated on potential types and methods of illicit appropriation, and the oversight process needs to include individuals knowledgeable about the innovation process.

The framework outlined in this chapter is one that is purposely not reliant on a traditional bureaucratic laced process; instead it is dependent on individuals working together to ensure society can reap the benefits of new technologies without worrying about potential revenge effects. As outlined by Wu, independent of the manner of regulation, whoever dictates the regulatory process will control innovation within an industry (its "master switch"). Despite the tendency to associate the term "regulation" with "government," Wu stipulates how a monopoly can exert the same control as a governmental body. Therefore, it is incumbent upon society to institute an effective and efficient manner of regulatory control over EDTs in order to prevent any one group from inhibiting future innovation development due to being risk adverse.[242]

> We have taught ourselves to create and combine the most powerful of technologies. We have not taken pains to learn about their consequences. Today these consequences threaten to destroy us. We must learn, and learn fast.[243]

[242] Wu, *The Master Switch*.

[243] Toffler, *Future Shock*, 440.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ambec, Stefan, Mark Cohen, Stewart Elgie, and Paul Lanoie. "The Porter Hypothesis at 20: Can Environmental Regulation Enhance Innovation and Competitiveness?" Resources for the Future. Accessed February 9, 2014. http://www.rff.org /documents/RFF-DP-11-01.pdf.

Anderson, Philip, and Michael Tushman. "Technological Discontinuities and Dominant Designs: A Cyclical Model of Technological Change." *Administrative Science Quarterly* 35, no. 4 (1990): 604–33. doi: 10.2307/2393511.

Ashford, Nicholas, ed. *National Support for Science & Technology: An Examination of Foreign Experience*. Cambridge: MIT Press, 1975.

Ashford, Nicholas, Christine Ayers and Robert Stone. "Using Regulation to Change the Market for Innovation." *Harvard Environmental Law Review* 9, no. 2 (1985): 419–66. http://hdl.handle.net/1721.1/1555.

Asur, Sitaram, and Bernardo Huberman. "Predicting the Future with Social Media." Hewlett Packard Development Company. Accessed June 13, 2014. http://www.hpl.hp.com/research/scl/papers /socialmedia/socialmedia.pdf.

Bass, Frank. "A New Product Growth Model for Consumer Durables." *Management Science* 15, no. 5 (1969): 215–27. doi:10.1287/mnsc.15.5.215

Boyd, Dallas, Lisa Andivahis, Jeffrey Cooper, Stephen Lukasik, Victor Oancea, and George Ullrich. *Revolutions in Science and Technology: Future Threats to U.S. National Security*. ASCO 2011-014. Washington, DC: Defense Threat Reduction Agency. Accessed February 10, 2014. http://www.hsdl.org/?view&did=706488.

Bright, James R. "Technology Forecasting Literature: Emergence and Impact on Technological Innovation." In *Technological Innovation: A Critical Review of Current Knowledge*, edited by Patrick Kelly and Melvin Kranzberg, 302–16. San Francisco: San Francisco Press, 1978.

Brynjolfsson, Erik and Andrew McAfee. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York: W.W. Norton & Company, 2014.

Chunara, Rumi, Jason Andrews, and John Brownstein. "Social and News Media Enable Estimation of Epidemiological Patterns Early in the 2010 Haitian Cholera Outbreak." *The American Society of Tropical Medicine and Hygiene* 86, no. 1 (2012): 39–45. doi: 10.4269/ajtmh.2012.11-0597.

Christensen, Clayton and Michael Overdorf. “Meeting the Challenge of Disruptive Change.” In *Harvard Business Review on Innovation*, 103–130. Boston: Harvard Business School Press, 2001.

Christensen, Clayton, and Michael Raynor. *The Innovator’s Solution: Creating and Sustaining Successful Growth*. Boston: Harvard Business School Press, 2003.

Christensen, Clayton. *The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harvard Business School Press, 1997.

Clark, Robert. *Intelligence Analysis: A Target-Centric Approach*. 4th ed. Washington DC: CQ Press, 2013.

Cohen, Manuel. “Cooperative Regulation.” Commission Speeches and Public Statements Archive, 1964. U.S. Securities and Exchange Commission. Last modified October 10, 2007. http://www.sec.gov/news/speech/speecharchive/1964speech.shtml.

Communication Department of the European Commission. “The Precautionary Principle.” Europa: Summaries of EU legislation. European Union. Last modified April 12, 2011. http://europa.eu/legislation_summaries/consumers/consumer_safety/l32042_en.htm.

“Connected Vehicles.” National Highway Traffic Safety Administration. Accessed March 11, 2014. http://icsw.nhtsa.gov/safercar/ConnectedVehicles/pages/v2v.html.

Coughlan, Peter, Nicholas Dew, and William Gates. “Crossing the Technology Adoption Chasm: Implications for DOD.” Monterey, CA: Naval Postgraduate School, 2008. http://www.acquisitionresearch.net/_files/FY2008/NPS-AM-08-116.pdf.

Denning, Peter. “The Science of Computing: The Internet Worm.” *American Scientist* 77, no. 2 (1989): 126–28. http://www.jstor.org/stable/27855650.

Director for Intelligence (J-2). *Joint Intelligence*. JP 2-0. Washington, DC: U.S. Government Printing Office, 2007. Accessed August 13, 2013. http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

Dix, Alan. “Designing for Appropriation.” *Proceedings of the BCS HCI 2007 Conference, People and Computers XXI*. London, UK: BCS-eWik. http://www.hcibook.com/alan/papers/HCI2007-appropriation/.

Duncan, Robert. “The Ambidextrous Organization: Designing Dual Structures for Innovation.” In *The Management of Organization Design, Vol. 1. Strategies and Implementation*, edited by Ralph Kilmann, Louis Pondy, and Dennis Slevin, 167–88. New York: North Holland, 1976.

Ellul, Jacques. *The Technological Bluff*. Grand Rapids, MI: W.B. Eerdmans, 1990.

Epstein, Richard. “Can Technological Innovation Survive Government Regulation?” *Harvard Journal of Law & Public Policy* 36, no. 1 (2013): 87–104. http://www.harvard-jlpp.com/wp-content/uploads/2013/01/36_1_087_Epstein_Tech.pdf.

Evans Heather. “Emerging Technologies IPC Has Inaugural Meeting.” Office of Science and Technology Policy, The White House. Last modified May 15, 2010. http://www.whitehouse.gov/blog/2010/05/15/emerging-technologies-ipc-has-inaugural-meeting.

“Facebook.” *Wikipedia*. Accessed June 13, 2014. http://en.wikipedia.org/wiki/Facebook.

Fenn, Jackie, and Mark Raskino. “Gartner’s Hype Cycle Special Report for 2013.” Gartner Insight. Gartner, Inc. Accessed February 11, 2014. http://my.gartner.com/portal/server.pt?open=512&objID=256&mode=2&PageID=2350940&resId=2574916.

Fenn, Jackie, and Mark Raskino. *Mastering the Hype Cycle: How to Choose the Right Innovation at the Right Time*. Boston: Harvard Business Press, 2008.

Hepburn, Glen. “Alternatives to Traditional Regulation.” Organization for Economic Co-operation and Development. Accessed February 6, 2014. http://www.oecd.org/gov/regulatory-policy/42245468.pdf.

Hoffman, Bruce. “Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post-Cold War Era.” *Intelligence and National Security* 11, no. 2. (1996): 207–23. doi: 10.1080/02684529608432353.

Gámez, Eduardo Calvillo and Rodrigo Nieto-Goméz. “The Case of ‘Illicit Appropriation’ in the Use of Technology.” In *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary* Perspectives, edited by Miguel Martin Vargas, Miguel A. Garcia-Ruiz, and Arthur Edwards, 210–29. Hershey, PA: Information Science Reference, 2011.

Grove, Andrew. *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career*. New York: Currency Doubleday, 1996.

“Inventor of the Week.” Lemelson-MIT. Massachusetts Institute of Technology. Last modified January 2002. http://web.mit.edu/invent/iow/ginsburg.html.

Kelly, Kevin. *What Technology Wants*. New York: Viking, 2010.

Kelly, Patrick and Melvin Kranzberg, ed. *Technological Innovation: A Critical Review of Current Knowledge*. San Francisco: San Francisco Press, 1978.

Kerbel, Josh. “The U.S. Intelligence Community’s Kodak Moment.” *The National Interest*. May 15, 2014. http://nationalinterest.org/feature/the-us-intelligence-communitys-kodak.

Kluckhuhn, Christopher. “An Examination of Four Successes in the Coast Guard’s Innovation Program and Implications for Innovation within Homeland Security.” Master’s thesis, Naval Postgraduate School, 2008. http://hdl.handle.net /10945/4216.

Kuchler, Hannah. “‘Heartbleed bug’ Threatens Web Traffic.” *Financial Times*, April 9, 2014. http://www.ft.com/intl/cms/s/0/89c12940-bf42-11e3-a4af -00144feabdc0.html.

“Listing of Federal Firearms Licensees (FFLs)—2014.” Bureau of Alcohol, Tobacco, Firearms and Explosives, United States Department of Justice. Accessed May 21, 2014. https://www.atf.gov/content/firearms/firearms-industry/listing-FFLs.

Lowenthal, Mark. *Intelligence: From Secrets to Policy*. 5th ed. Los Angeles: Sage Publications, 2012.

Lowenthal, Mark. “Towards a Reasonable Standard for Analysis.” *Intelligence and National Security* 23, no. 3 (2008): 303–15, doi: 10.1080/02684520802121190.

Lustick, Ian. *Trapped in the War on Terror*. Philadelphia: University of Pennsylvania Press, 2006.

Marchant, Gary Elvin, Kenneth W. Abbott, and Braden R. Allenby, ed. *Innovative Governance Models for Emerging Technologies*. Northampton, PA: Edward Elgar Publishing, 2013.

Markay, Lachlan. “Pentagon Paid $150 Per Gallon for Green Jet Fuel: Report.” *The Washington Times*, May 7, 2014. http://www.washingtontimes.com/.

McCraw, Thomas K. “American Capitalism.” In *Creating Modern Capitalism: How Entrepreneurs, Companies, and Countries Triumphed in Three Industrial Revolutions*, edited by Thomas K. McCraw, 303–48. Cambridge: Harvard University Press, 1998.

McGrath, Rita, and Ian MacMillan. “Discovery-Driven Planning.” *Harvard Business Review* 73, no. 4 (1995): 44–54. http://hbr.org/1995/07/discovery-driven -planning/.

Moore, Geoffrey. *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers*. New York: HarperBusiness, 1999.

Morison, Elting. *Men, Machines, and Modern Times*. Cambridge, MA: M.I.T. Press, 1966.

Nieto-Goméz, Rodrigo. “Power of ‘the Few’ A Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment.” *Homeland Security Affairs* 7, no. 18 (2011): 2–21. http://hdl.handle.net/10945/24994.

———. “Preventing the Next 9/10 The Homeland Security Challenges of Technological Evolution and Convergence in the Next Ten Years.” *Homeland Security Affairs* 7, (2011): 1–6. http://hdl.handle.net/10945/24988.

“Office of Technology Assessment Act,” The Technology Assessment Act. The Trustees of Princeton University. Accessed June 23, 2014, http://www.princeton.edu/~ota/ns20/act_f.html.

“The Origin of the Bass Model.” Bass’s Basement Research Institute. Accessed March 11, 2014. http://www.bassbasement.org/BassModel/Default.aspx.

Phaal, Robert, Clare Farrukh, and David Probert. “Technology Roadmapping—A Planning Framework for Evolution and Revolution.” *Technological Forecasting & Social Change* 71, (2004): 5–26. doi: 10.1016/S0040-1625(03)00072-6.

Porter, Michael, and Claas van der Linde. “Toward a New Conception of the Environment-Competitiveness Relationship.” *The Journal of Economic Perspectives* 9, no. 4 (1995): 97–118. http://www.jstor.org/stable/2138392.

Rasmussen, Maria, and Mohammad Hafez. “Terrorist Innovations in Weapons of Mass Effect: Preconditions, Causes and Predictive Indicators.” ASCO 2010-019. Washington, DC: Defense Threat Reduction Agency. Accessed February 10, 2014. http://www.nps.edu/Academics/Centers/CCC/Research/2010%20019%20Terrorist%20Innovations%20in%20WME.pdf.

Rogers, Everett. *Diffusion of Innovations*. 5th ed. New York: Free Press, 2003.

Schelling, Thomas. *Micromotives and Macrobehavior*. New York: Norton, 1978.

Schumpeter, Joseph. *Capitalism, Socialism, and Democracy*. New York: Harper, 1950.

“Science and Technology Special Programs Division.” U.S. Department of Homeland Security. Accessed May 21, 2014. http://www.dhs.gov/st-special-programs-division.

Singleton, Solveig. “Regulatory Obstacles to Innovation: Is Self-Regulation the Answer?” CATO Institute. Accessed Feb. 2, 2014. http://www.cato.org/pubs/wtpapers/990913catoself.html.

Segal, Howard. *Future Imperfect: The Mixed Blessings of Technology in America*. Amherst, MA: University of Massachusetts Press, 1994.

“Segway—The Leader in Personal, Green Transportation.” Segway, Inc. Accessed March 11, 2014. http://www.segway.com.

"Social Physics: A New Way of Understanding Human Behavior Based on Analysis of Big Data." MIT Media Lab. Accessed August 5, 2014. http://socialphysics.media.mit.edu.

Stewart, Luke. "The Impact of Regulation on Innovation in the United States: A Cross-Industry Literature Review." Commissioned paper for the Institute of Medicine Committee on Patient Safety and Health IT. 2010. Accessed February 9, 2014. http://www.iom.edu/~/media/Files/Report%20Files/2011/Health-IT/Commissioned-paper-Impact-of-Regulation-on-Innovation.pdf.

Stewart, Richard. "Regulation, Innovation, and Administrative Law: A Conceptual Framework." *California Law Review* 69, no. 5 (1981): 1256–377. http://www.jstor.org/stable/3480247.

Stinson, Benjamin. "Understanding How Program Managers Successfully Manage Innovation in Major Defense Acquisition Programs (MDAPs): An Exploratory Study." Master's thesis, Naval Postgraduate School, 2001. http://hdl.handle.net/10945/10817.

Stoneman, Paul, and Paul Diederen. "Technology Diffusion and Public Policy." *The Economic Journal* 104, no. 425 (1994): 918-30. http://www.jstor.org/stable/2234987.

Stoneman, Paul. *Handbook of the Economics of Innovations and Technological Change*. Oxford, UK: Blackwell, 1995.

Sunstein, Cass. "The Paralyzing Principle." *Regulation* (2002): 32–7. http://object.cato.org/sites/cato.org/files/serials/files/regulation/2002/12/v25n4-9.pdf

Tenner, Edward. *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*. New York: Knopf, 1996.

Thomke, Stefan. "Enlightened Experimentation: The New Imperative for Innovation." *Harvard Business Review* 79, no. 2 (2001). (Reprinted in Harvard Business Review on Innovation. Boston, MA: Harvard Business School Press, 2001.)

Report of the National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Official government ed. Washington, DC: U.S. Government Printing Office, 2004.

Toffler, Alvin. *Future Shock*. New York: Random House, 1970.

Tucker, Jonathan. *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. Cambridge, MA: MIT Press, 2012.

Tushman, Michael, and Charles O'Reilly. *Winning Through Innovation: A Practical Guide to Leading Organizational Change and Renewal*. Boston: Harvard Business School Press, 1997.

Tushman, Michael, and Philip Anderson. "Technological Discontinuities and Organizational Environments." *Administrative Science Quarterly* 31, no. 3 (1986): 439–65. doi: 10.2307/2392832.

Utterback, James, and Linsu Kim. "Invasion of a Stable Business by Radical Innovation." In *The Management of Productivity and Technology in Manufacturing*, edited by Paul Kleindorfer, 113–51. New York: Plenum Press, 1985. http://dx.doi.org /10.1007/978-1-4613-2507-9_5.

Utterback, James, and William Abernathy. "A Dynamic Model of Product and Process Innovation." *Omega* 3, no. 6 (1975): 639–56. doi: 10.1016/0305-0483(75) 90068-7.

Waterman, Robert. *Adhocracy: The Power to Change*. New York: W.W. Norton, 1992.

Wiener, Jonathan. "The Regulation of Technology, and the Technology of Regulation." *Technology in Society* 26, (2004): 483–500. doi: 10.1016/j.techsoc.2004.01.033.

Wu, Tim. *The Master Switch: The Rise and Fall of Information Empires*. New York: Alfred A. Knopf, 2010.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California